AT-IX5-28GPX

HIGH AVAILABILITY, HIGH POWER VIDEO SURVEILLANCE PoE SWITCH

Command Reference for AlliedWare Plus™ Version 5.4.6-0.x

the solution : the network

C613-50086-01 REV A

Acknowledgments

Contents

List of Commands

Part 1: Setup and Troubleshooting

1 CLI Navigation Commands

Introduction

Overview This chapter provides an alphabetical reference for the commands used to navigate between different modes. This chapter also provides a reference for the help and show commands used to help navigate within the CLI.

Command List

configure terminal

Overview This command enters the Global Configuration command mode.

Syntax

```
configure terminal
```

Mode Privileged Exec

Example To enter the Global Configuration command mode (note the change in the command prompt), enter the command:

```
awplus# configure terminal
awplus(config)#
```

disable (Privileged Exec mode)

Overview This command exits the Privileged Exec mode, returning the prompt to the User Exec mode. To end a session, use the exit command.

Syntax

```
disable
```

Mode Privileged Exec

Example To exit the Privileged Exec mode, enter the command:

```
awplus# disable
awplus>
```

Related Commands

enable (Privileged Exec mode)

end

exit

do

Overview This command lets you to run User Exec and Privileged Exec mode commands when you are in any configuration mode.

Syntax

```
do <command>
```

Parameter	Description
<command>	Specify the command and its parameters.

Mode Any configuration mode

Example

```
awplus# configure terminal
awplus(config)# do ping 192.0.2.23
```

enable (Privileged Exec mode)

Overview This command enters the Privileged Exec mode and optionally changes the privilege level for a session. If a privilege level is not specified then the maximum privilege level (15) is applied to the session. If the optional privilege level is omitted then only users with the maximum privilege level can access Privileged Exec mode without providing the password as specified by the enable password or enable secret commands. If no password is specified then only users with the maximum privilege level set with the username command can assess Privileged Exec mode.

Syntax

```
enable [<privilege-level>]
```

Parameter	Description
<privilege-level>	Specify the privilege level for a CLI session in the range <1-15>, where 15 is the maximum privilege level, 7 is the intermediate privilege level and 1 is the minimum privilege level. The privilege level for a user must match or exceed the privilege level set for the CLI session for the user to access Privileged Exec mode. Privilege level for a user is configured by username.

Mode User Exec

Usage Many commands are available from the Privileged Exec mode that configure operating parameters for the device, so you should apply password protection to the Privileged Exec mode to prevent unauthorized use. Passwords can be encrypted but then cannot be recovered. Note that non-encrypted passwords are shown in plain text in configurations.

The username command sets the privilege level for the user. After login, users are given access to privilege level 1. Users access higher privilege levels with the enable (Privileged Exec mode) command. If the privilege level specified is higher than the users configured privilege level specified by the username command, then the user is prompted for the password for that level.

Note that a separate password can be configured for each privilege level using the enable password and the enable secret commands from the Global Configuration mode. The service password-encryption command encrypts passwords configured by the enable password and the enable secret commands, so passwords are not shown in plain text in configurations.

Example The following example shows the use of the **enable** command to enter the Privileged Exec mode (note the change in the command prompt).

```
awplus> enable
awplus#
```

The following example shows the **enable** command enabling access the Privileged Exec mode for users with a privilege level of 7 or greater. Users with a privilege level of 7 or greater do not need to enter a password to access Privileged Exec mode. Users with a privilege level 6 or less need to enter a password to access

Privilege Exec mode. Use the enable password command or the enable secret commands to set the password to enable access to Privileged Exec mode.

```
awplus> enable 7
awplus#
```

Related Commands

disable (Privileged Exec mode)

enable password

enable secret

exit

service password-encryption

username

end

Overview This command returns the prompt to the Privileged Exec command mode from any other advanced command mode.

Syntax

```
end
```

Mode All advanced command modes, including Global Configuration and Interface Configuration modes.

Example The following example shows the use of the `end` command to return to the Privileged Exec mode directly from Interface mode.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# end
awplus#
```

Related Commands

disable (Privileged Exec mode)

enable (Privileged Exec mode)

exit

exit

Overview This command exits the current mode, and returns the prompt to the mode at the previous level. When used in User Exec mode, the **exit** command terminates the session.

Syntax

```
exit
```

Mode All command modes, including Global Configuration and Interface Configuration modes.

Example The following example shows the use of `exit` command to exit Interface mode, and return to Configure mode.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# exit
awplus(config)#
```

Related Commands

disable (Privileged Exec mode)

enable (Privileged Exec mode)

end

help

Overview This command displays a description of the AlliedWare Plus™ OS help system.

Syntax `help`

Mode All command modes

Example To display a description on how to use the system help, use the command:

```
awplus# help
```

Output Figure 1-1: Example output from the **help** command

```
When you need help at the command line, press '?'.

If nothing matches, the help list will be empty. Delete
characters until entering a '?' shows the available options.

Enter '?' after a complete parameter to show remaining valid
command parameters (e.g. 'show ?').

Enter '?' after part of a parameter to show parameters that
complete the typed letters (e.g. 'show ip?').
```

logout

Overview This command exits the User Exec or Privileged Exec modes and ends the session.

Syntax

```
logout
```

Mode User Exec and Privileged Exec

Example To exit the User Exec mode, use the command:

```
awplus# logout
```

show history

Overview This command lists the commands entered in the current session. The history buffer is cleared automatically upon reboot.

The output lists all command line entries, including commands that returned an error.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show history
```

Mode User Exec and Privileged Exec

Example To display the commands entered during the current session, use the command:

```
awplus# show history
```

Output Figure 1-2: Example output from the **show history** command

```
1 en
2 show ru
3 conf t
4 route-map er deny 3
5 exit
6 ex
7 di
```

2 File Management Commands

Introduction

This chapter provides an alphabetical reference of AlliedWare Plus™ OS file management commands.

Filename Syntax and Keyword Usage

Many of the commands in this chapter use the placeholder "filename" to represent the name and location of the file that you want to act on. The following table explains the syntax of the filename for each different type of file location.

When you copy a file...	Use this syntax:	Example:
Copying in local Flash memory	`flash:[/][<directory>/]<filename>`	To specify a file in the configs directory in Flash: flash:configs/example.cfg
Copying to or from a USB storage device	`usb:[/][<directory>/]<filename>`	To specify a file in the top-level directory of the USB stick: usb:example.cfg
Copying with HTTP	`http://[[<username>:<password>]@]{<hostname>|<host-ip>}[/<filepath>]/<filename>`	To specify a file in the configs directory on the server: http://www.company.com/configs/example.cfg
Copying with TFTP	`tftp://[[<location>]/<directory>]/<filename>`	To specify a file in the top-level directory of the server: tftp://172.1.1.1/example.cfg
Copying with SCP	`scp://<username>@<location>[/<directory>][/<filename>]`	To specify a file in the configs directory on the server, logging on as user "bob": e.g. scp://bob@10.10.0.12/configs/example.cfg

When you copy a file...	Use this syntax:	Example:
Copying with SFTP	`sftp://[[<location>]/<directory>]/<filename>`	To specify a file in the top-level directory of the server: sftp://10.0.0.5/example.cfg
Copying to or from stack member Flash	`<hostname>-<stack_ID>/flash:[/][<directory>/]<stack_member_filename>`	To specify a file in the configs directory on member 2 of a stack named vcstack: vcstack-2/flash:/configs/example.cfg

Valid characters

The filename and path can include characters from up to four categories. The categories are:

1) uppercase letters: A to Z
2) lowercase letters: a to z
3) digits: 0 to 9
4) special symbols: all printable ASCII characters not included in the previous three categories. Including the following characters:
   - -
   - /
   - .
   - _
   - @
   - "
   - '
   - *
   - :
   - ~
   - ?

Do not use spaces or parentheses within filenames. Use hyphens or underscores instead.

Syntax for directory listings

A leading slash (/) indicates the root of the current filesystem location.

In commands where you need to specify the local filesystem's Flash base directory, you may use **flash** or **flash:** or **flash:/**. For example, these commands are all the same:

- `dir flash`
- `dir flash:`
- `dir flash:/`

Similarly, you can specify the USB storage device base directory with **usb** or **usb:** or **usb:/**

You cannot name a directory or subdirectory **flash**, **nvs**, **usb**, **card**, **tftp**, **scp**, **sftp** or **http.** These keywords are reserved for tab completion when using various file commands.

In a stacked environment you can only access `flash` and `nvs` using the stack member filepath (e.g. `dir awplus-2/flash:/`). To access a USB storage device on a backup stack member, use the remote-login command.

Command List

autoboot enable

Overview This command enables the device to restore a release file and/or a configuration file from external media, such as a USB storage device.

When the Autoboot feature is enabled, the device looks for a special file called `autoboot.txt` on the external media. If this file exists, the device will check the key and values in the file and recover the device with a new release file and/or configuration file from the external media. An example of a valid `autoboot.txt` file is shown in the following figure.

Figure 2-1: Example autoboot.txt file

```
[AlliedWare Plus]
Copy_from_external_media_enabled=yes
Boot_Release=IX5-5.4.6-0.1.rel
Boot_Config=network1.cfg
```

Use the **no** variant of this command to disable the Autoboot feature.

NOTE: *This command is not supported in a stacked configuration.*

Syntax

```
autoboot enable
no autoboot enable
```

Default The Autoboot feature operates the first time the device is powered up in the field, after which the feature is disabled by default.

Mode Global Configuration

Example To enable the Autoboot feature, use the command:

```
awplus# configure terminal
awplus# configure terminal
awplus(config)# no autoboot enable
```

Related Commands

create autoboot

show autoboot

show boot

boot config-file

Overview Use this command to set the configuration file to use during the next boot cycle.

Use the **no** variant of this command to remove the configuration file.

Syntax

```
boot config-file <filepath-filename>
no boot config-file
```

Parameter	Description
<filepath-filename>	Filepath and name of a configuration file. The specified configuration file must exist in the specified filesystem. Valid configuration files must have a **.cfg** extension.

Mode Global Configuration

Usage You can only specify that the configuration file is on a USB storage device if there is a backup configuration file already specified in Flash. If you attempt to set the configuration file on a USB storage device and a backup configuration file is not specified in Flash, the following error message is displayed:

```
% Backup configuration files must be stored in the flash
filesystem
```

For an explanation of the configuration fallback order, see the File Management Feature Overview and Configuration Guide.

Examples To run the configuration file `branch.cfg` stored on the device's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot config-file flash:/branch.cfg
```

To remove the configuration file `branch.cfg` stored on the device's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# no boot config-file flash:/branch.cfg
```

To run the configuration file `branch.cfg` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot config-file usb:/branch.cfg
```

To remove the configuration file `branch.cfg` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# no boot config-file usb:/branch.cfg
```

Related Commands

boot config-file backup

boot system

boot system backup

show boot

boot config-file backup

Overview Use this command to set a backup configuration file to use if the main configuration file cannot be accessed.

Use the **no** variant of this command to remove the backup configuration file.

Syntax

```
boot config-file backup <filepath-filename>
no boot config-file backup
```

Parameter	Description
<filepath-filename>	Filepath and name of a backup configuration file. Backup configuration files must be in the Flash filesystem. Valid backup configuration files must have a **.cfg** extension.
`backup`	The specified file is a backup configuration file.

Mode Global Configuration

Usage For an explanation of the configuration fallback order, see the File Management Feature Overview and Configuration Guide.

Examples To set the configuration file `backup.cfg` as the backup to the main configuration file, use the commands:

```
awplus# configure terminal
awplus(config)# boot config-file backup flash:/backup.cfg
```

To remove the configuration file `backup.cfg` as the backup to the main configuration file, use the commands:

```
awplus# configure terminal
awplus(config)# no boot config-file backup flash:/backup.cfg
```

Related Commands

boot config-file

boot system

boot system backup

show boot

boot system

Overview Use this command to set the release file to load during the next boot cycle.

Use the **no** variant of this command to remove the release file as the boot file.

Syntax

```
boot system <filepath-filename>
no boot system
```

Parameter	Description
<filepath-filename>	Filepath and name of a release file. The specified release file must exist and must be stored in the root directory of the specified filesystem. Valid release files must have a **.rel** extension.

Mode Global Configuration

Usage You can only specify that the release file is on a USB storage device if there is a backup release file already specified in Flash. If you attempt to set the release file on a USB storage device and a backup release file is not specified in Flash, the following error message is displayed:

```
% A backup boot image must be set before setting a current boot
image on USB storage device
```

In a VCStack configuration, the stack only accepts a release file on a USB storage device if a USB storage device is inserted in all stack members and all stack members have a bootloader version that supports booting from it. If a stack member has a USB storage device removed an error message is displayed. For example, if stack member 2 does not have a USB storage device inserted the following message is displayed:

```
% Stack member 2 has no USB storage device inserted
```

Examples To run the release file `IX5-5.4.6-0.1.rel` stored on the device's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system flash:/IX5-5.4.6-0.1.rel
```

To remove the release file `IX5-5.4.6-0.1.rel` stored on the device's Flash filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system flash:/IX5-5.4.6-0.1.rel
```

To run the release file `IX5-5.4.6-0.1.rel` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system usb:/IX5-5.4.6-0.1.rel
```

To remove the release file `IX5-5.4.6-0.1.rel` stored on the switch's USB storage device filesystem the next time the device boots up, use the commands:

```
awplus# configure terminal
awplus(config)# boot system usb:/IX5-5.4.6-0.1.rel
```

In a VCStack configuration, if there is not enough space to synchronize the new release across the stack, the boot system command has an interactive mode that prompts you to delete old releases.

```
awplus# configure terminal
awplus(config)# boot system IX5-5.4.6-0.1.rel
```

```
Insufficient flash available on stack member-2 (11370496)
 to synchronize file IX5-5.4.6-0.1.rel
(14821895).

 List of release files on stack member-2
         IX5-5.4.6-0.1.rel (14822400)

 Select files to free up space,
 Delete awplus-2/flash:/IX5-5.4.6-0.1.rel
? (y/n)[n]:y
```

```
awplus(config)# y
```

```
 Deleting selected files, please wait.........................
 Successful operation
 VCS synchronizing file across the stack, please wait.............
 File synchronization with stack member-2 successfully completed
 [DONE]
```

Related Commands

boot config-file

boot config-file backup

boot system backup

show boot

boot system backup

Overview Use this command to set a backup release file to load if the main release file cannot be loaded.

Use the **no** variant of this command to remove the backup release file as the backup boot file.

Syntax

```
boot system backup <filepath-filename>
no boot system backup
```

Parameter	Description
<filepath-filename>	Filepath and name of a backup release file. Backup release files must be in the Flash filesystem. Valid release files must have a **.rel** extension.
`backup`	The specified file is a backup release file.

Mode Global Configuration

Examples To specify the file `IX5-5.4.6-0.1.rel` as the backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# boot system backup flash:/IX5-5.4.6-0.1.rel
```

To remove the file `IX5-5.4.6-0.1.rel` as the backup to the main release file, use the commands:

```
awplus# configure terminal
awplus(config)# no boot system backup flash:/IX5-5.4.6-0.1.rel
```

Related Commands

boot config-file

boot config-file backup

boot system

show boot

cd

Overview This command changes the current working directory.

Syntax

```
cd <directory-name>
```

Parameter	Description
<directory-name>	Name and path of the directory.

Mode Privileged Exec

Example To change to the directory called `images`, use the command:

```
awplus# cd images
```

Related Commands

dir

pwd

show file systems

copy (filename)

Overview This command copies a file. This allows you to:

- copy files from your device to a remote device
- copy files from a remote device to your device
- copy files stored on Flash memory to or from a different memory type, such as a USB storage device
- create two copies of the same file on your device

Syntax

```
copy <source-name> <destination-name>
```

Parameter	Description
<source-name>	The filename and path of the source file. See Introduction on page 82 for valid syntax.
<destination-name>	The filename and path for the destination file. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Examples To use TFTP to copy the file `bob.key` into the current directory from the remote server at `10.0.0.1`, use the command:

```
awplus# copy tftp://10.0.0.1/bob.key bob.key
```

To use SFTP to copy the file `new.cfg` into the current directory from a remote server at `10.0.1.2`, use the command:

```
awplus# copy sftp://10.0.1.2/new.cfg bob.key
```

To use SCP with the username `beth` to copy the file `old.cfg` into the directory `config_files` on a remote server that is listening on TCP port 2000, use the command:

```
awplus# copy scp://beth@serv:2000/config_files/old.cfg old.cfg
```

To copy the file `newconfig.cfg` onto your device's Flash from a USB storage device, use the command:

```
awplus# copy usb:/newconfig.cfg flash:/newconfig.cfg
```

To copy the file `newconfig.cfg` to a USB storage device from your device's Flash, use the command:

```
awplus# copy flash:/newconfig.cfg usb:/newconfig.cfg
```

To copy the file `config.cfg` into the current directory from a USB storage device, and rename it to `configtest.cfg`, use the command:

```
awplus# copy usb:/config.cfg configtest.cfg
```

To copy the file `config.cfg` into the current directory from a remote file server, and rename it to `configtest.cfg`, use the command:

```
awplus# copy fserver:/config.cfg configtest.cfg
```

To copy the file `test.txt` from the top level of Flash on stack member 2 to the current directory in the stack master, use the command:

```
awplus# copy awplus-2/flash:/test.txt test.txt
```

Note that you must specify either the NVS or Flash filesystem on the (backup) stack member (`flash`: in this example).

Related Commands

copy zmodem

edit (filename)

show file systems

copy current-software

Overview This command copies the AlliedWare Plus™ OS software that the device has booted from, to a destination file. Specify whether the destination is Flash or USB when saving the software to the local filesystem.

Syntax

```
copy current-software <destination-name>
```

Parameter	Description
<destination-name>	The filename and path where you would like the current running-release saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Example To copy the current software as installed in the working directory with the file name `my-release.rel`, use the command:

```
awplus# copy current-software my-release.rel
```

Related Commands

boot system backup

show boot

copy debug

Overview This command copies a specified debug file to a destination file. Specify whether the destination is Flash or USB when saving the software to the local filesystem.

Syntax

```
copy debug {<destination-name>|debug|flash|nvs|scp|tftp|usb}
{<source-name>|debug|flash|nvs|scp|tftp|usb}
```

Parameter	Description
<destination-name>	The filename and path where you would like the debug output saved. See Introduction on page 82 for valid syntax.
<source-namee>	The filename and path where the debug output originates. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Example To copy debug output to a USB storage device with a filename `my-debug`, use the following command:

```
awplus# copy debug usb:my-debug
```

Output Figure 2-2: CLI prompt after entering the **copy debug** command

```
Enter source file name []:
```

Related Commands

delete debug

move debug

copy running-config

Overview This command copies the running-config to a destination file, or copies a source file into the running-config. Commands entered in the running-config do not survive a device reboot unless they are saved in a configuration file.

Syntax

```
copy <source-name> running-config
copy running-config [<destination-name>]
copy running-config startup-config
```

Parameter	Description
<source-name>	The filename and path of a configuration file. This must be a valid configuration file with a **.cfg** filename extension. Specify this when you want the script in the file to become the new running-config. See Introduction on page 82 for valid syntax.
<destination-name>	The filename and path where you would like the current running-config saved. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See Introduction on page 82 for valid syntax. If you do not specify a file name, the device saves the running-config to a file called default.cfg.
`startup-config`	Copies the running-config into the file set as the current startup-config file.

Mode Privileged Exec

Examples To copy the `running-config` into the startup-config, use the command:

```
awplus# copy running-config startup-config
```

To copy the file `layer3.cfg` into the `running-config`, use the command:

```
awplus# copy layer3.cfg running-config
```

To use SCP to copy the running-config as `current.cfg` to the remote server listening on TCP port 2000, use the command:

```
awplus# copy running-config
scp://user@server:2000/config_files/current.cfg
```

Related Commands

copy startup-config

write file

write memory

copy startup-config

Overview This command copies the startup-config script into a destination file, or alternatively copies a configuration script from a source file into the startup-config file. Specify whether the destination is Flash or USB when loading from the local filesystem.

Syntax

```
copy <source-name> startup-config
copy startup-config <destination-name>
```

Parameter	Description
<source-name>	The filename and path of a configuration file. This must be a valid configuration file with a **.cfg** filename extension. Specify this to copy the script in the file into the startup-config file. Note that this does not make the copied file the new startup file, so any further changes made in the configuration file are not added to the startup-config file unless you reuse this command. See Introduction on page 82 for valid syntax.
<destination-name>	The destination and filename that you are saving the startup- config as. This command creates a file if no file exists with the specified filename. If a file already exists, then the CLI prompts you before overwriting the file. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Examples To copy the file `Layer3.cfg` to the `startup-config`, use the command:

```
awplus# copy Layer3.cfg startup-config
```

To copy the `startup-config` as the file `oldconfig.cfg` in the current directory, use the command:

```
awplus# copy startup-config oldconfig.cfg
```

Related Commands copy running-config

copy zmodem

Overview This command allows you to copy files using ZMODEM using Minicom. ZMODEM works over a serial connection and does not need any interfaces configured to do a file transfer.

Syntax

```
copy <source-name> zmodem
copy zmodem
```

Parameter	Description
<source-name>	The filename and path of the source file. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Example To copy the local file `asuka.key` using ZMODEM, use the command:

```
awplus# copy asuka.key zmodem
```

Related Commands copy (filename)

show file systems

create autoboot

Overview Use this command to create an `autoboot.txt` file on external media. This command will automatically ensure that the keys and values that are expected in this file are correct. After the file is created the **create autoboot** command will copy the current release and configuration files across to the external media. The external media is then available to restore a release file and/or a configuration file to the device.

Syntax

```
create autoboot [usb]
```

Mode Privileged Exec

Example To create an `autoboot.txt` file on external media, use the command:

```
awplus# create autoboot usb
```

Related Commands

autoboot enable

show autoboot

show boot

delete

Overview This command deletes files or directories.

Syntax `delete [force] [recursive] <filename>`

Parameter	Description
`force`	Ignore nonexistent filenames and never prompt before deletion.
`recursive`	Remove the contents of directories recursively.
`<filename>`	The filename and path of the file to delete. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Examples To delete the file `temp.cfg` from the current directory, use the command:

```
awplus# delete temp.cfg
```

To delete the read-only file `one.cfg` from the current directory, use the command:

```
awplus# delete force one.cfg
```

To delete the directory `old_configs`, which is not empty, use the command:

```
awplus# delete recursive old_configs
```

To delete the directory `new_configs`, which is not empty, without prompting if any read-only files are being deleted, use the command:

```
awplus# delete force recursive new_configs
```

Related Commands erase startup-config

rmdir

delete debug

Overview Use this command to delete a specified debug output file.

Syntax

```
delete debug <source-name>
```

Parameter	Description
<source-name>	The filename and path where the debug output originates. See Introduction on page 82 for valid URL syntax.

Mode Privileged Exec

Example To delete debug output, use the following command:

```
awplus# delete debug
```

Output Figure 2-3: CLI prompt after entering the **delete debug** command

```
Enter source file name []:
```

Related Commands

copy debug

move debug

dir

Overview This command lists the files on a filesystem. If no directory or file is specified then this command lists the files in the current working directory.

Syntax
```
dir [all] [recursive] [sort [reverse] [name|size|time]]
[<filename>|debug|flash|nvs|usb]
```

Parameter	Description
`all`	List all files.
`recursive`	List the contents of directories recursively.
`sort`	Sort directory listing.
`reverse`	Sort using reverse order.
`name`	Sort by name.
`size`	Sort by size.
`time`	Sort by modification time (default).
<filename>	The name of the directory or file. If no directory or file is specified, then this command lists the files in the current working directory.
`debug`	Debug root directory
`flash`	Flash memory root directory
`nvs`	NVS memory root directory
`usb`	USB storage device root directory

Mode Privileged Exec

Usage In a stacked environment you can use the CLI on a stack master to access filesystems that are located on another stack member. The syntax is *<hostname>*`-`*<stack_ID>*`/flash:[/][`*<directory>*`/]`*<stack_member_filename>*. For example, to specify a file in the configs directory on member 2 of a stack, enter:

```
awplus-2/flash:/configs/example.cfg
```

Examples To list the files in the current working directory, use the command:

```
awplus# dir
```

To list the non-hidden files in the root of the Flash filesystem, use the command:

```
awplus# dir flash
```

To list all the files in the root of the Flash filesystem, use the command:

```
awplus# dir all flash:
```

To list recursively the files in the Flash filesystem, use the command:

```
awplus# dir recursive flash:
```

To list the files in alphabetical order, use the command:

```
awplus# dir sort name
```

To list the files by size, smallest to largest, use the command:

```
awplus# dir sort reverse size
```

To sort the files by modification time, oldest to newest, use the command:

```
awplus# dir sort reverse time
```

To list the files within the Flash filesystem for stack member 2, use the command:

```
awplus# dir awplus-2/flash:/
```

Note that you must specify the filesystem on the stack member (`flash` in this example).

Related Commands

cd

pwd

edit

Overview This command opens a text file in the AlliedWare Plus™ text editor. Once opened you can use the editor to alter to the file.

If a filename is specified and it already exists, then the editor opens it in the text editor.

If no filename is specified, the editor prompts you for one when you exit it.

Before starting the editor make sure your terminal, terminal emulation program, or Telnet client is 100% compatible with a VT100 terminal. The editor uses VT100 control sequences to display text on the terminal.

For more information about using the editor, including control sequences, see the File Management Feature Overview and Configuration Guide.

Syntax

```
edit [<filename>]
```

Parameter	Description
<filename>	Name of a file in the local Flash filesystem.

Mode Privileged Exec

Examples To create and edit a new text file, use the command:

```
awplus# edit
```

To edit the existing configuration file `myconfig.cfg` stored on your device's Flash memory, use the command:

```
awplus# edit myconfig.cfg
```

Related Commands edit (filename)

show file

edit (filename)

Overview This command opens a remote text file as read-only in the AlliedWare Plus™ text editor.

Before starting the editor make sure your terminal, terminal emulation program, or Telnet client is 100% compatible with a VT100 terminal. The editor uses VT100 control sequences to display text on the terminal.

Syntax

```
edit <filename>
```

Parameter	Description
<filename>	The filename and path of the remote file. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Example To view the file `bob.key` stored in the security directory of a TFTP server, use the command:

```
awplus# edit tftp://security/bob.key
```

Related Commands

copy (filename)

edit

show file

erase startup-config

Overview This command deletes the file that is set as the startup-config file, which is the configuration file that the system runs when it boots up.

At the next restart, the device loads the default configuration file, default.cfg. If default.cfg no longer exists, then the device loads with the factory default configuration. This provides a mechanism for you to return the device to the factory default settings.

Syntax

```
erase startup-config
```

Mode Privileged Exec

Example To delete the file currently set as the startup-config, use the command:

```
awplus# erase startup-config
```

Related Commands

boot config-file backup

copy running-config

copy startup-config

show boot

ip tftp source-interface

Overview Use this command to manually specify the IP address that all TFTP requests originate from. This is useful in network configurations where TFTP servers only accept requests from certain devices, or where the server cannot dynamically determine the source of the request.

Use the **no** variant of this command to stop specifying a source.

Syntax

```
ip tftp source-interface [<interface>|<ip-add>]
no ip tftp source-interface
```

Parameter	Description
<interface>	The VLAN that TFTP requests originate from. The device will use the IP address of this interface as its source IP address.
<ip-add>	The IP address that TFTP requests originate from, in dotted decimal format

Default There is no default source specified.

Mode Global Configuration

Usage This command is helpful in network configurations where TFTP traffic needs to traverse point-to-point links or subnets within your network, and you do not want to propagate those point-to-point links through your routing tables.

In those circumstances, the TFTP server cannot dynamically determine the source of the TFTP request, and therefore cannot send the requested data to the correct device. Specifying a source interface or address enables the TFTP server to send the data correctly.

Example To specify that TFTP requests originate from the IP address 192.0.2.1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip tftp source-interface 192.0.2.1
```

Related Commands copy (filename)

ipv6 tftp source-interface

Overview Use this command to manually specify the IPv6 address that all TFTP requests originate from. This is useful in network configurations where TFTP servers only accept requests from certain devices, or where the server cannot dynamically determine the source of the request.

Use the **no** variant of this command to stop specifying a source.

Syntax

```
ipv6 tftp source-interface [<interface>|<ipv6-add>]
no ipv6 tftp source-interface
```

Parameter	Description
<interface>	The VLAN that TFTP requests originate from. The device will use the IPv6 address of this interface as its source IPv6 address.
<ipv6-add>	The IPv6 address that TFTP requests originate from, in the format x:x::x:x, for example, 2001:db8::8a2e:7334.

Default There is no default source specified.

Mode Global Configuration

Usage This command is helpful in network configurations where TFTP traffic needs to traverse point-to-point links or subnets within your network, and you do not want to propagate those point-to-point links through your routing tables.

In those circumstances, the TFTP server cannot dynamically determine the source of the TFTP request, and therefore cannot send the requested data to the correct device. Specifying a source interface or address enables the TFTP server to send the data correctly.

Example To specify that TFTP requests originate from the IPv6 address 2001:db8::8a2e:7334, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 tftp source-interface 2001:db8::8a2e:7334
```

Related Commands copy (filename)

mkdir

Overview This command makes a new directory.

Syntax

```
mkdir <name>
```

Parameter	Description
<name>	The name and path of the directory that you are creating.

Mode Privileged Exec

Usage You cannot name a directory or subdirectory **flash**, **nvs**, **usb**, **card**, **tftp**, **scp**, **sftp** or **http.** These keywords are reserved for tab completion when using various file commands.

Example To make a new directory called `images` in the current directory, use the command:

```
awplus# mkdir images
```

Related Commands

cd

dir

pwd

move

Overview This command renames or moves a file.

Syntax

```
move <source-name> <destination-name>
```

Parameter	Description
<source-name>	The filename and path of the source file. See Introduction on page 82 for valid syntax.
<destination-name>	The filename and path of the destination file. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Examples To rename the file `temp.cfg` to `startup.cfg`, use the command:

```
awplus# move temp.cfg startup.cfg
```

To move the file `temp.cfg` from the root of the Flash filesystem to the directory `myconfigs`, use the command:

```
awplus# move temp.cfg myconfigs/temp.cfg
```

Related Commands

delete

edit

show file

show file systems

move debug

Overview This command moves a specified debug file to a destination debug file.

Syntax

```
move debug {<destination-name>|debug|flash|nvs|usb}
{<source-name>|debug|flash|nvs|usb}
```

Parameter	Description
<destination-name>	The filename and path where you would like the debug output moved to. See Introduction on page 82 for valid syntax.
<source-name>	The filename and path where the debug output originates. See Introduction on page 82 for valid syntax.

Mode Privileged Exec

Example To move debug output onto a USB storage device with a filename `my-debug`, use the following command:

```
awplus# move debug usb:my-debug
```

Output Figure 2-4: CLI prompt after entering the **move debug** command

```
Enter source file name []:
```

Related Commands

copy debug

delete debug

pwd

Overview This command prints the current working directory.

Syntax

```
pwd
```

Mode Privileged Exec

Example To print the current working directory, use the command:

```
awplus# pwd
```

Related Commands cd

rmdir

Overview This command removes a directory. This command only works on empty directories, unless you specify the optional **force** keyword.

Syntax

```
rmdir [force] <name>
```

Parameter	Description
`force`	Optional keyword that allows you to delete directories that are not empty and contain files or subdirectories.
<name>	The name and path of the directory.

Mode Privileged Exec

Usage In a stacked environment you can use the CLI on a stack master to access filesystems that are located on another stack member. See the Introduction on page 82 for syntax details.

Examples To remove the directory `images` from the top level of the Flash filesystem, use the command:

```
awplus# rmdir flash:/images
```

To create a directory called `level1` containing a subdirectory called `level2`, and then force the removal of both directories, use the commands:

```
awplus# mkdir level1
awplus# mkdir level1/level2
awplus# rmdir force level1
```

To remove a directory called `test` from the top level of the Flash filesystem, in stack member 3, use the command:

```
awplus# rmdir awplus-3/flash:/test
```

Note that you must specify the filesystem, ("flash:" in this example).

Related Commands

cd

dir

mkdir

pwd

show autoboot

Overview This command displays the Autoboot configuration and status.

Syntax

```
show autoboot
```

Mode Privileged Exec

Example To show the Autoboot configuration and status, use the command:

```
awplus# show autoboot
```

Output Figure 2-5: Example output from the **show autoboot** command

```
awplus#show autoboot
Autoboot configuration
------------------------------------------------------------------------------
Autoboot status                  : enabled
USB file autoboot.txt exists     : yes

Restore information on USB
Autoboot enable in autoboot.txt  : yes
Restore release file             : IX5-5.4.6-0.1.rel
(file exists)
Restore configuration file       : network_1.cfg (file exists)
```

Figure 2-6: Example output from the **show autoboot** command when an external media source is not present

```
awplus#show autoboot
Autoboot configuration
------------------------------------------------------------------------------
Autoboot status                  : enabled
External media source            : USB not found.
```

Related Commands

autoboot enable

create autoboot

show boot

show boot

Overview This command displays the current boot configuration. We recommend that the currently running release is set as the current boot image.

Syntax

```
show boot
```

Mode Privileged Exec

Example To show the current boot configuration, use the command:

```
awplus# show boot
```

Output Figure 2-7: Example output from the **show boot** command when the current boot config is on a USB storage device

```
awplus#show boot
Boot configuration
-----------------------------------------------------------------
Current software   : IX5-5.4.6-0.1.rel
Current boot image : usb:/IX5-5.4.6-0.1.rel
Backup  boot image : flash:/IX5-5.4.5-2.1.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/my.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file not found)
Autoboot status    : enabled
```

Table 1: Parameters in the output of the **show boot** command

Parameter	Description
`Current software`	The current software release that the device is using.
`Current boot image`	The boot image currently configured for use during the next boot cycle.
`Backup boot image`	The boot image to use during the next boot cycle if the device cannot load the main image.
`Default boot config`	The default startup configuration file. The device loads this configuration script if no file is set as the startup-config file.
`Current boot config`	The configuration file currently configured as the startup-config file. The device loads this configuration file during the next boot cycle if this file exists.

Table 1: Parameters in the output of the **show boot** command (cont.)

Parameter	Description
`Backup boot config`	The configuration file to use during the next boot cycle if the main configuration file cannot be loaded.
`Autoboot status`	The status of the Autoboot feature; either enabled or disabled.

Related Commands

autoboot enable

boot config-file backup

boot system backup

show autoboot

show file

Overview This command displays the contents of a specified file.

Syntax

```
show file <filename>
```

Parameter	Description
<filename>	Name of a file on the local Flash filesystem, or name and directory path of a file.

Mode Privileged Exec

Example To display the contents of the file `oldconfig.cfg`, which is in the current directory, use the command:

```
awplus# show file oldconfig.cfg
```

Related Commands

edit

edit (filename)

show file systems

show file systems

Overview This command lists the filesystems and their utilization information where appropriate.

If this command is entered on the stack master, it will list the filesystems for all the stack members. A stack member heading is displayed to distinguish the different lists shown for each stack member.

Syntax

```
show file systems
```

Mode Privileged Exec

Examples To display the filesystems for either a standalone device, or a complete stack, use the command:

```
awplus# show file systems
```

Output Figure 2-8: Example output from the **show file systems** command

```
awplus#show file systems
 Size(b)   Free(b)   Type    Flags  Prefixes   S/D/V    Lcl/Ntwk  Avail
-----------------------------------------------------------------------
  63.0M     29.4M   flash     rw  flash:     static  local      Y
     -         -   system    rw  system:    virtual local      -
  10.0M      9.9M   debug     rw  debug:     static  local      Y
 499.0K    404.0K   nvs       rw  nvs:       static  local      Y
     -         -   usbstick  rw  usb:       dynamic local      N
     -         -   tftp      rw  tftp:      -       network    -
     -         -   scp       rw  scp:       -       network    -
     -         -   sftp      ro  sftp:      -       network    -
     -         -   http      ro  http:      -       network    -
     -         -   rsync     rw  rsync:     -       network    -
```

Table 2: Parameters in the output of the **show file systems** command

Parameter	Description
`Size (B)` `Available`	The total memory available to this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.
`Free (B)`	The total memory free within this filesystem. The units are given after the value and are M for Megabytes or k for kilobytes.

Table 2: Parameters in the output of the **show file systems** command (cont.)

Parameter	Description
`Type`	The memory type used for this filesystem; one of: flash system nvs usbstick tftp scp sftp http.
`Flags`	The file setting options: rw (read write), ro (read only).
`Prefixes`	The prefixes used when entering commands to access the filesystems; one of: flash system nvs usb tftp scp sftp http.
`S/V/D`	The memory type: static, virtual, dynamic.
`Lcl / Ntwk`	Whether the memory is located locally or via a network connection.
`Avail`	Whether the memory is accessible: Y (yes), N (no), - (not applicable)

Related Commands

edit

edit (filename)

show file

show running-config

Overview This command displays the current configuration of your device. Its output includes all non-default configuration. The default settings are not displayed.

You can control the output in the following ways:

- To display only lines that contain a particular word, enter the following parameters after the command:

  `| include <word>`

- To start the display at the first line that contains a particular word, enter the following parameters after the command:

  `| begin <word>`

- To save the output to a file, enter the following parameters after the command:

  `> <filename>`

Syntax `show running-config`

Mode Privileged Exec and Global Configuration

Example To display the current configuration of your device, use the command:

```
awplus# show running-config
```

Output Figure 2-9: Example output from the **show running-config** command

```
awplus#show running-config
!
service password-encryption
!
hostname MyNode
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
autoboot enable
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
snmp-server contact Documentation Area
snmp-server location New Zealand
```

```
!
aaa authentication enable default local
aaa authentication login default local
!
ip domain-lookup
!
no service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
switch 1 provision IX5-28
!
vlan database
 vlan 2-15 state enable
!
interface port1.0.1-1.0.6
 switchport
 switchport mode access
!
interface port1.0.25-1.0.26
 switchport
 switchport mode access
 switchport access vlan 14
!
interface vlan1
 ip address 192.168.1.1/24
 ipv6 enable
 ipv6 mld
!
interface vlan12
 ip address 192.168.3.1/24!
ipv6 forwarding
!
line con 0
line vty 0 4
!
end
```

Related Commands copy running-config

show running-config access-list

Overview Use this command to show the running system status and configuration details for access-list.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show running-config access-list
```

Mode Privileged Exec and Global Configuration

Example To display the running system status and configuration details for access-list, use the command:

```
awplus# show running-config access-list
```

Output Figure 2-10: Example output from the s**how running-config access-list** command

```
!
access-list abc remark annai
access-list abc deny any
access-list abd deny any
!
```

Related Commands

copy running-config

show running-config

show running-config as-path access-list

Overview Use this command to show the running system status and configuration details for as-path access-list.

Syntax

```
show running-config as-path access-list
```

Mode Privileged Exec and Global Configuration

Example To display the running system status and configuration details for as-path access-list, use the command:

```
awplus# show running-config as-path access-list
```

Output Figure 2-11: Example output from the **show running-config as-path access-list** command

```
!
ip as-path access-list wer permit knsmk
!
```

Related Commands

copy running-config

show running-config

show running-config dhcp

Overview Use this command to display the running configuration for DHCP server, DHCP snooping, and DHCP relay.

Syntax

```
show running-config dhcp
```

Mode Privileged Exec and Global Configuration

Example To display to display the running configuration for DHCP server, DHCP snooping, and DHCP relay:

```
awplus# show running-config dhcp
```

Output Figure 2-12: Example output from the **show running-config dhcp** command

```
awplus#show running-config dhcp
no service dhcp-server
!
service dhcp-snooping
!
interface port1.0.1
 ip dhcp snooping trust
!
interface port1.0.3
 ip dhcp snooping max-bindings 25
 access-group dhcpsnooping
interface port1.0.4
 ip dhcp snooping max-bindings 25
 access-group dhcpsnooping
!
interface po1
 ip dhcp snooping max-bindings 25
 arp security violation log
!
interface sa1
 ip dhcp snooping max-bindings 25
 access-group dhcpsnooping
 arp security violation log
!
interface vlan100
 ip dhcp snooping
 arp security
!
interface vlan200
 ip dhcp snooping
 arp security
!
```

Related Commands

copy running-config

show running-config

show running-config full

Overview Use this command to show the complete status and configuration of the running system.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show running-config full
```

Mode Privileged Exec and Global Configuration

Example To display the complete status and configuration of the running system, use the command:

```
awplus# show running-config full
```

Output Figure 2-13: Example output from the **show running-config full** command

```
awplus#show running-config full
!
service password-encryption
!
hostname MyNode
!
no banner motd
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
autoboot enable
!
service telnet
!
service http
!
no clock timezone
!
snmp-server
snmp-server contact Documentation Area
snmp-server location New Zealand
```

```
!
aaa authentication enable default local
aaa authentication login default local
!
ip domain-lookup
!
no service dhcp-server
!
no ip multicast-routing
!
spanning-tree mode rstp
!
switch 1 provision IX5-28
!
vlan database
 vlan 2-15 state enable
!
interface port1.0.1-1.0.6
 switchport
 switchport mode access
!
interface port1.0.25-1.0.26
 switchport
 switchport mode access
 switchport access vlan 14
!
interface vlan1
 ip address 192.168.1.1/24
 ipv6 enable
 ipv6 mld
!
interface vlan12
 ip address 192.168.3.1/24!
ipv6 forwarding
!
line con 0
line vty 0 4
!
end
```

Related Commands

copy running-config

show running-config

show running-config interface

Overview This command displays the current configuration of one or more interfaces on the device.

Syntax

```
show running-config interface [<interface-list>] [dot1x|ip
igmp|lacp|mstp|rstp|stp]
```

Parameter	Description
<interface-list>	The interfaces or ports to display information about. An interface-list can be: • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen, e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`dot1x`	Displays running configuration for 802.1X port authentication for the specified interfaces.
`lacp`	Displays running configuration for LACP (Link Aggregation Control Protocol) for the specified interfaces.
`ip igmp`	Displays running configuration for IGMP (Internet Group Management Protocol) for the specified interfaces.
`ip multicast`	Displays running configuration for general multicast settings for the specified interfaces.
`mstp`	Displays running configuration for MSTP (Multiple Spanning Tree Protocol) for the specified interfaces.
`rstp`	Displays running configuration for RSTP (Rapid Spanning Tree Protocol) for the specified interfaces.
`stp`	Displays running configuration for STP (Spanning Tree Protocol) for the specified interfaces.

Mode Privileged Exec and Global Configuration

Examples To display the current running configuration of your device for ports 1 to 4, use the command:

```
awplus# show running-config interface port1.0.1-port1.0.4
```

To display the current running configuration of a device for VLAN 1, use the command:

```
awplus# show running-config interface vlan1
```

To display the current running configuration of a device for VLANs 1 and 3-5, use the command:

```
awplus# show running-config interface vlan1,vlan3-vlan5
```

Output Figure 2-14: Example output from a **show running-config interface** port1.0.2 command

```
awplus#sh running-config interface port1.0.2
!
interface port1.0.2
 switchport
 switchport mode access
!
```

Figure 2-15: Example output from the **show running-config interface** command

```
awplus#show running-config interface
interface port1.0.1-1.0.6
 switchport
 switchport mode access
!
interface port1.0.25-1.0.26
 switchport
 switchport mode access
 switchport access vlan 14
!
interface port1.0.27-1.0.28
 switchport
 switchport mode access
 switchport access vlan 15
!
interface vlan1
 ip address 192.168.1.1/24
 ipv6 enable
 ipv6 mld
!
interface vlan12
 ip address 192.168.3.1/24
!
interface vlan13
 ip address 192.168.2.1/24
```

Related Commands

copy running-config

show running-config

show running-config ip route

Overview Use this command to show the running system static IPv4 route configuration.

For information on filtering and saving command output, see "Controlling "show" Command Output" of the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show running-config ip route
```

Mode Privileged Exec and Global Configuration

Example To display the running system static IPv4 route configuration, use the command:

```
awplus# show running-config ip route
```

Output Figure 2-16: Example output from the **show running-config ip route** command

```
!
ip route 3.3.3.3/32 vlan3
ip route 3.3.3.3/32 vlan2
!
```

Related Commands

copy running-config

show running-config

show running-config ipv6 access-list

Overview Use this command to show the running system status and configuration for IPv6 ACLs.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show running-config ipv6 access-list
```

Mode Privileged Exec and Global Configuration

Example To display the running system status and configuration for IPv6 ACLs, use the command:

```
awplus# show running-config ipv6 access-list
```

Output Figure 2-17: Example output from the **show running-config ipv6 access-list** command

```
!
ipv6 access-list abc permit any
!
```

Related Commands

copy running-config

show running-config

show running-config ipv6 route

Overview Use this command to show the running system static IPv6 route configuration.

For information on filtering and saving command output, see "Controlling "show" Command Output" of the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show running-config ipv6 route
```

Mode Privileged Exec and Global Configuration

Example To display the running system static IPv6 route configuration, use the command:

```
awplus# show running-config ipv6 route
```

Output Figure 2-18: Example output from the **show running-config ipv6 route** command

```
!
ipv6 route 3e11::/64 lo
ipv6 route 3e11::/64 vlan2
ipv6 route fe80::/64 vlan3
!
```

Related Commands

copy running-config

show running-config

show running-config key chain

Overview Use this command to show the running system key-chain related configuration.

Syntax

```
show running-config key chain
```

Mode Privileged Exec and Global Configuration

Example To display the running system key-chain related configuration, use the command:

```
awplus# show running-config key chain
```

Output Figure 2-19: Example output from the **show running-config key chain** command

```
!
key chain 12
key 2
key-string 234
!
key chain 123
key 3
key-string 345
!
```

Related Commands

copy running-config

show running-config

show running-config lldp

Overview This command shows the current running configuration of LLDP.

Syntax

```
show running-config lldp
```

Mode Privileged Exec and Global Configuration

Example To display the current configuration of LLDP, use the command:

```
awplus# show running-config lldp
```

Output Figure 2-20: Example output from the **show running-config lldp** command

```
awplus#show running-config lldp

lldp notification-interval 10
lldp timer 20
!
interface port1.0.1
 lldp notifications
 lldp tlv-select port-description
 lldp tlv-select system-name
 lldp tlv-select system-description
 lldp tlv-select management-address
 lldp transmit receive
```

Related Commands

show lldp

show lldp interface

show running-config power-inline

Overview Use this command to show the Power over Ethernet (PoE) running system status and configuration details. The PoE usage-threshold percentage as specified by the power-inline usage-threshold command is displayed in the **running-config** using this command.

Syntax

```
show running-config power-inline
```

Mode Privileged Exec and Global Configuration

Example To display the PoE running system status and configuration details, use the command:

```
awplus# show running-config power-inline
```

Output Figure 2-21: Example output from the **show running-config power-inline** command

```
!
power-inline usage-threshold 90
!
```

Related Commands power-inline usage-threshold

show power-inline

show running-config route-map

Overview Use this command to show the running system status and configuration details for route-map.

For information on filtering and saving command output, see "Controlling "show" Command Output" of the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show running-config route-map
```

Mode Privileged Exec and Global Configuration

Example To display the running system status and configuration details for route-map, use the command:

```
awplus# show running-config route-map
```

Output Figure 2-22: Example output from the **show running-config route-map** command

```
!
route-map abc deny 2
match community 2
!
route-map abc permit 3
match route-type external type-2
set metric-type type-1
!
```

Related Commands

copy running-config

show running-config

show running-config router

Overview Use the show running-config router command to display the current running configuration for a given router.

Syntax

```
show running-config router <protocol>
```

Parameter	Description
<protocol>	ospf | rip |ipv6 rip | vrrp
ospf	Open Shortest Path First (OSPF)
rip	Routing Information Protocol (RIP)
ipv6 rip	IPv6 RIP
vrrp	Virtual Redundancy Routing Protocol (VRRP)

Mode Privileged Exec and Global Configuration

Example To display the current running configuration for a given router, use the command:

```
awplus# show running-config router ospf
```

Output Figure 2-23: Example output from the **show running-config router** command

```
!
router ospf
 network 192.168.1.0/24 area 0.0.0.0
 network 192.168.3.0/24 area 0.0.0.0
!
```

Related Commands

copy running-config

show running-config

show running-config router-id

Overview Use this command to show the running system global router ID configuration.

Syntax

```
show running-config router-id
```

Mode Privileged Exec and Global Configuration

Example To display the running system global router ID configuration, use the command:

```
awplus# show running-config router-id
```

Output Figure 2-24: Example output from the **show running-config router-id** command

```
!
router-id 3.3.3.3
!
```

Related Commands

copy running-config

show running-config

show running-config security-password

Overview This command displays the configuration settings for the various security-password rules. If a default parameter is used for a security-password rule, therefore disabling that rule, no output is displayed for that feature.

Syntax

```
show running-config security-password
```

Mode Privileged Exec and Global Configuration

Example To display the current security-password rule settings in the running-config, use the command:

```
awplus# show running-config security-password
```

Output Figure 2-25: Example output from the **show running-config security-password** command

```
security-password minimum-length 8
security-password minimum-categories 3
security-password history 4
security-password lifetime 30
security-password warning 3
security-password forced-change
```

Related Commands

show security-password configuration

show security-password user

show startup-config

Overview This command displays the contents of the start-up configuration file, which is the file that the device runs on start-up.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show startup-config
```

Mode Privileged Exec

Example To display the contents of the current start-up configuration file, use the command:

```
awplus# show startup-config
```

Output Figure 2-26: Example output from the **show startup-config** command

```
awplus#show startup-config
!
service password-encryption
!
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
!
no service ssh
!
service telnet
!
service http
!
no clock timezone
.
.
.
line con 0
line vty 0 4
!
end
```

Related Commands

boot config-file backup

copy running-config

copy startup-config

erase startup-config

show boot

show version

Overview This command displays the version number and copyright details of the current AlliedWare Plus™ OS your device is running.

Syntax

```
show version
```

Mode User Exec and Privileged Exec

Example To display the version details of your currently installed software, use the command:

```
awplus# show version
```

Related Commands

boot system backup

show boot

write file

Overview This command copies the running-config into the file that is set as the current startup-config file. This command is a synonym of the **write memory** and **copy running-config startup-config** commands.

Syntax

```
write [file]
```

Mode Privileged Exec

Example To write configuration data to the start-up configuration file, use the command:

```
awplus# write file
```

Related Commands

copy running-config

write memory

show running-config

write memory

Overview This command copies the running-config into the file that is set as the current startup-config file. This command is a synonym of the **write file** and **copy running-config startup-config** commands.

Syntax

```
write [memory]
```

Mode Privileged Exec

Example To write configuration data to the start-up configuration file, use the command:

```
awplus# write memory
```

Related Commands

copy running-config

write file

show running-config

write terminal

Overview This command displays the current configuration of the device. This command is a synonym of the show running-config command.

Syntax

```
write terminal
```

Mode Privileged Exec

Example To display the current configuration of your device, use the command:

```
awplus# write terminal
```

Related Commands show running-config

3 User Access Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure user access.

Command List

clear line console

Overview This command resets a console line. If a terminal session exists on the line then the terminal session is terminated. If console line settings have changed then the new settings are applied.

Syntax
```
clear line console 0
```

Mode Privileged Exec

Example To reset the console line (asyn), use the command:

```
awplus# clear line console 0
awplus# % The new settings for console line 0 have been applied
```

Related Commands
clear line vty

flowcontrol hardware (asyn/console)

line

show users

clear line vty

Overview This command resets a VTY line. If a session exists on the line then it is closed.

Syntax

```
clear line vty <0-32>
```

Parameter	Description
<0-32>	Line number

Mode Privileged Exec

Example To reset the first vty line, use the command:

```
awplus# clear line vty 1
```

Related Commands

privilege level

line

show telnet

show users

enable password

Overview To set a local password to control access to various privilege levels, use the enable password Global Configuration command. Use the enable password command to modify or create a password to be used, and use the no enable password command to remove the password.

Note that the enable secret command is an alias for the enable password command, and the no enable secret command is an alias for the no enable password command. Issuing a no enable password command removes a password configured with the enable secret command. The enable password command is shown in the running and startup configurations. Note that if the enable secret command is entered then enable password is shown in the configuration.

NOTE: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

Syntax

```
enable password [<plain>|8 <hidden>|level <1-15> 8 <hidden>]
no enable password [level <1-15>]
```

Parameter	Description
`<plain>`	Specifies the unencrypted password.
`8`	Specifies a hidden password will follow.
`<hidden>`	Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.
`level`	Privilege level <1-15>. Level for which the password applies. You can specify up to 16 privilege levels, using numbers 1 through 15. Level 1 is normal EXEC-mode user privileges for User Exec mode. If this argument is not specified in the command or the **no** variant of the command, the privilege level defaults to 15 (enable mode privileges) for Privileged Exec mode. A privilege level of 7 can be set for intermediate CLI security.

Default The privilege level for enable password is level 15 by default. Previously the default was level 1.

Mode Global Configuration

Usage This command enables the Network Administrator to set a password for entering the Privileged Exec mode when using the enable (Privileged Exec mode) command. There are three methods to enable a password. In the examples below, for each method, note that the configuration is different and the configuration file output is different, but the password string to be used to enter the Privileged Exec mode with the **enable** command is the same (**mypasswd**).

A user can now have an intermediate CLI security level set with this command for privilege level 7 to access all the show commands in Privileged Exec mode and all

the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.

Note that the enable password command is an alias for the enable secret command and one password per privilege level is allowed using these commands. Do not assign one password to a privilege level with enable password and another password to a privilege level with enable secret. Use enable password or enable secret commands. Do not use both on the same level.

Using plain passwords

The plain password is a clear text string that appears in the configuration file as configured.

```
awplus# configure terminal
awplus(config)# enable password mypasswd
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password mypasswd
!
interface lo
```

Using encrypted passwords

You can configure an encrypted password using the service password-encryption command. First, use the enable password command to specify the string that you want to use as a password (**mypasswd**). Then, use the service password-encryption command to encrypt the specified string (**mypasswd**). The advantage of using an encrypted password is that the configuration file does not show **mypasswd**, it will only show the encrypted string **fU7zHzuutY2SA**.

NOTE: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

```
awplus# configure terminal
awplus(config)# enable password mypasswd
awplus(config)# service password-encryption
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
service password-encryption
!
interface lo
```

Using hidden passwords

You can configure an encrypted password using the **HIDDEN** parameter (**8**) with the enable password command. Use this method if you already know the encrypted string corresponding to the plain text string that you want to use as a

password. It is not required to use the service password-encryption command for this method. The output in the configuration file will show only the encrypted string, and not the text string.

```
awplus# configure terminal
awplus(config)# enable password 8 fU7zHzuutY2SA
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
!
interface lo
```

Related Commands

enable (Privileged Exec mode)

enable secret

service password-encryption

privilege level

show privilege

username

show running-config

enable secret

Overview To set a local password to control access to various privilege levels, use the enable secret Global Configuration command. Use the enable secret command to modify or create a password to be used, and use the no enable secret command to remove the password.

Note that the enable secret command is an alias for the enable password command, and the no enable secret command is an alias for the no enable password command. Issuing a no enable password command removes a password configured with the enable secret command. The enable password command is shown in the running and startup configurations. Note that if the enable secret command is entered then enable password is shown in the configuration.

NOTE: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

Syntax

```
enable secret [<plain>|8 <hidden>|level <0-15> 8 <hidden>]
no enable secret [level <1-15>]
```

Parameter	Description
`<plain>`	Specifies the unencrypted password.
`8`	Specifies a hidden password will follow.
`<hidden>`	Specifies the hidden encrypted password. Use an encrypted password for better security where a password crosses the network or is stored on a TFTP server.
`level`	Privilege level <1-15>. Level for which the password applies. You can specify up to 16 privilege levels, using numbers 1 through 15. Level 1 is normal EXEC-mode user privileges for User Exec mode. If this argument is not specified in the command or the **no** variant of the command, the privilege level defaults to 15 (enable mode privileges) for Privileged Exec mode. A privilege level of 7 can be set for intermediate CLI security.

Default The privilege level for enable secret is level 15 by default.

Mode Global Configuration

Usage This command enables the Network Administrator to set a password for entering the Privileged Exec mode when using the enable (Privileged Exec mode) command. There are three methods to enable a password. In the examples below, for each method, note that the configuration is different and the configuration file output is different, but the password string to be used to enter the Privileged Exec mode with the **enable** command is the same (**mypasswd**).

A user can have an intermediate CLI security level set with this command for privilege level 7 to access all the show commands in Privileged Exec mode and all

the commands in User Exec mode, but not any configuration commands in Privileged Exec mode.

Note that the enable secret command is an alias for the enable password command and one password per privilege level is allowed using these commands. Do not assign one password to a privilege level with enable password and another password to a privilege level with enable secret. Use enable password or enable secret commands. Do not use both on the same level.

Using plain passwords

The plain password is a clear text string that appears in the configuration file as configured.

```
awplus# configure terminal
awplus(config)# enable secret mypasswd
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password mypasswd
!
interface lo
```

Using encrypted passwords

Configure an encrypted password using the service password-encryption command. First, use the enable password command to specify the string that you want to use as a password (**mypasswd**). Then, use the service password-encryption command to encrypt the specified string (**mypasswd**). The advantage of using an encrypted password is that the configuration file does not show **mypasswd**, it will only show the encrypted string **fU7zHzuutY2SA**.

NOTE: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

```
awplus# configure terminal
awplus(config)# enable secret mypasswd
awplus(config)# service password-encryption
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
service password-encryption
!
interface lo
```

Using hidden passwords

Configure an encrypted password using the **HIDDEN** parameter (**8**) with the **enable password** command. Use this method if you already know the encrypted string corresponding to the plain text string that you want to use as a password. It

is not required to use the service password-encryption command for this method. The output in the configuration file will show only the encrypted string, and not the text string:

```
awplus# configure terminal
awplus(config)# enable secret 8 fU7zHzuutY2SA
awplus(config)# end
```

This results in the following show output:

```
awplus#show run
Current configuration:
hostname awplus
enable password 8 fU7zHzuutY2SA
!
interface lo
```

Related Commands

enable (Privileged Exec mode)

enable secret

service password-encryption

privilege level

show privilege

username

show running-config

exec-timeout

Overview This command sets the interval your device waits for user input from either a console or VTY connection. Once the timeout interval is reached, the connection is dropped. This command sets the time limit when the console or VTY connection automatically logs off after no activity.

The **no** variant of this command removes a specified timeout and resets to the default timeout (10 minutes).

Syntax

```
exec-timeout {<minutes>} [<seconds>]
no exec-timeout
```

Parameter	Description
<minutes>	<0-35791> Required integer timeout value in minutes
<seconds>	<0-2147483> Optional integer timeout value in seconds

Default The default for the **exec-timeout** command is 10 minutes and 0 seconds (**exec-timeout 10 0**).

Mode Line Configuration

Usage This command is used set the time the telnet session waits for an idle VTY session, before it times out. An **exec-timeout 0 0** setting will cause the telnet session to wait indefinitely. The command **exec-timeout 0 0** is useful while configuring a device, but reduces device security.

If no input is detected during the interval then the current connection resumes. If no connections exist then the terminal returns to an idle state and disconnects incoming sessions.

Examples To set VTY connections to timeout after 2 minutes, 30 seconds if there is no response from the user, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# exec-timeout 2 30
```

To reset the console connection to the default timeout of 10 minutes 0 seconds if there is no response from the user, use the following commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no exec-timeout
```

Validation Commands show running-config

Related Commands

line

service telnet

flowcontrol hardware (asyn/console)

Overview Use this command to enable RTS/CTS (Ready To Send/Clear To Send) hardware flow control on a terminal console line (asyn port) between the DTE (Data Terminal Equipment) and the DCE (Data Communications Equipment).

Syntax

```
flowcontrol hardware
no flowcontrol hardware
```

Mode Line Configuration

Default Hardware flow control is disabled by default.

Usage Hardware flow control makes use of the RTS and CTS control signals between the DTE and DCE where the rate of transmitted data is faster than the rate of received data. Flow control is a technique for ensuring that a transmitting entity does not overwhelm a receiving entity with data. When the buffers on the receiving device are full, a message is sent to the sending device to suspend the transmission until the data in the buffers has been processed.

Hardware flow control can be configured on terminal console lines (e.g. asyn0). For Reverse Telnet connections, hardware flow control must be configured to match on both the Access Server and the Remote Device. For terminal console sessions, hardware flow control must be configured to match on both the DTE and the DCE. Settings are saved in the running configuration. Changes are applied after reboot, clear line console, or after closing the session.

Use **show running-config** and **show startup-config** commands to view hardware flow control settings that take effect after reboot for a terminal console line. See the **show running-config** command output:

```
awplus#show running-config
!
line con 1
  speed 9600
  mode out 2001
  flowcontrol hardware
!
```

Note that line configuration commands do not take effect immediately. Line configuration commands take effect after one of the following commands or events:

- issuing a clear line console command
- issuing a reboot command
- logging out of the current session

Examples

To enable hardware flow control on terminal console line asyn0, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# flowcontrol hardware
```

To disable hardware flow control on terminal console line asyn0, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no flowcontrol hardware
```

Related Commands

clear line console

show running-config

speed (asyn)

length (asyn)

Overview Use this command to specify the number of rows of output that the device will display before pausing, for the console or VTY line that you are configuring.

The **no** variant of this command restores the length of a line (terminal session) attached to a console port or to a VTY to its default length of 22 rows.

Syntax

```
length <0-512>
no length
```

Parameter	Description
<0-512>	Number of lines on screen. Specify 0 for no pausing.

Mode Line Configuration

Default The length of a terminal session is 22 rows. The **no length** command restores the default.

Usage If the output from a command is longer than the length of the line the output will be paused and the '–More–' prompt allows you to move to the next screen full of data.

A length of 0 will turn off pausing and data will be displayed to the console as long as there is data to display.

Examples To set the terminal session length on the console to 10 rows, use the command:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# length 10
```

To reset the terminal session length on the console to the default (22 rows), use the command:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# no length
```

To display output to the console continuously, use the command:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# length 0
```

Related Commands terminal resize

terminal length

line

Overview Use this command to enter line configuration mode for the specified VTYs or the console. The command prompt changes to show that the device is in Line Configuration mode.

Syntax

```
line vty <first-line> [<last-line>]
line console 0
```

Parameter	Description
<first-line>	*<0-32>* Specify the first line number.
<last-line>	*<0-32>* Specify the last line number.
console	The console terminal line(s) for local access.
vty	Virtual terminal for remote console access.

Mode Global Configuration

Usage In Line Configuration mode, you can configure console and virtual terminal settings, including setting speed (asyn), length (asyn), privilege level, and authentication (login authentication) or accounting (accounting login) method lists.

To change the console (asyn) port speed, use this **line** command to enter Line Configuration mode before using the speed (asyn) command. Set the console speed (Baud rate) to match the transmission rate of the device connected to the console (asyn) port on your device.

Note that line configuration commands do not take effect immediately. Line configuration commands take effect after one of the following commands or events:

- issuing a clear line console command
- issuing a reboot command
- logging out of the current session

Examples To enter Line Configuration mode in order to configure all VTYs, use the commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)#
```

To enter Line Configuration mode to configure the console (asyn 0) port terminal line, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)#
```

Related Commands

accounting login

clear line console

clear line vty

flowcontrol hardware (asyn/console)

length (asyn)

login authentication

privilege level

speed (asyn)

privilege level

Overview This command sets a privilege level for VTY or console connections. The configured privilege level from this command overrides a specific user's initial privilege level at the console login.

Syntax

```
privilege level <1-15>
```

Mode Line Configuration

Usage You can set an intermediate CLI security level for a console user with this command by applying privilege level 7 to access all show commands in Privileged Exec and all User Exec commands. However, intermediate CLI security will not show configuration commands in Privileged Exec.

Examples To set the console connection to have the maximum privilege level, use the following commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# privilege level 15
```

To set all vty connections to have the minimum privilege level, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# privilege level 1
```

To set all vty connections to have an intermediate CLI security level, to access all show commands, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 5
awplus(config-line)# privilege level 7
```

Related Commands

enable password

line

show privilege

username

security-password history

Overview This command specifies the number of previous passwords that are unable to be reused. A new password is invalid if it matches a password retained in the password history.

The **no security-password history** command disables the security password history functionality.

Syntax

```
security-password history <0-15>
no security-password history
```

Parameter	Description
<0-15>	The allowable range of previous passwords to match against. A value of *0* will disable the history functionality and is equivalent to the **no security-password history** command. If the history functionality is disabled, all users' password history is reset and all password history is lost.

Default The default history value is `0`, which will disable the history functionality.

Mode Global Configuration

Examples To restrict reuse of the three most recent passwords, use the command:

```
awplus# configure terminal
awplus(config)# security-password history 3
```

To allow the reuse of recent passwords, use the command:

```
awplus# configure terminal
awplus(config)# no security-password history
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password forced-change

security-password lifetime

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

security-password forced-change

Overview This command specifies whether or not a user is forced to change an expired password at the next login. If this feature is enabled, users whose passwords have expired are forced to change to a password that must comply with the current password security rules at the next login.

Note that to use this command, the lifetime feature must be enabled with the security-password lifetime command and the reject-expired-pwd feature must be disabled with the security-password reject-expired-pwd command.

The **no security-password forced-change** command disables the forced-change feature.

Syntax

```
security-password forced-change
no security-password forced-change
```

Default The forced-change feature is disabled by default.

Mode Global Configuration

Example To force a user to change their expired password at the next login, use the command:

```
awplus# configure terminal
awplus(config)# security-password forced-change
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password history

security-password lifetime

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

security-password lifetime

Overview This command enables password expiry by specifying a password lifetime in days.

Note that when the password lifetime feature is disabled, it also disables the security-password forced-change command and the security-password warning command.

The **no security-password lifetime** command disables the password lifetime feature.

Syntax

```
security-password lifetime <0-1000>
no security-password lifetime
```

Parameter	Description
<0-1000>	Password lifetime specified in days. A value of *0* will disable lifetime functionality and the password will never expire. This is equivalent to the **no security-password lifetime** command.

Default The default password lifetime is `0`, which will disable the lifetime functionality.

Mode Global Configuration

Example To configure the password lifetime to 10 days, use the command:

```
awplus# configure terminal
awplus(config)# security-password lifetime 10
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password history

security-password forced-change

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

security-password warning

show security-password user

security-password minimum-categories

Overview This command specifies the minimum number of categories that the password must contain in order to be considered valid. The password categories are:

- uppercase letters: A to Z
- lowercase letters: a to z
- digits: 0 to 9
- special symbols: all printable ASCII characters not included in the previous three categories. The question mark (?) cannot be used as it is reserved for help functionality.

Note that to ensure password security, the minimum number of categories should align with the lifetime selected, i.e. the fewer categories specified the shorter the lifetime specified.

Syntax

```
security-password minimum-categories <1-4>
```

Parameter	Description
<1-4>	Number of categories the password must satisfy, in the range 1 to 4.

Default The default number of categories that the password must satisfy is `1`.

Mode Global Configuration

Example To configure the required minimum number of character categories to be `3`, use the command:

```
awplus# configure terminal
awplus(config)# security-password minimum-categories 3
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password history

security-password forced-change

security-password lifetime

security-password minimum-length

security-password reject-expired-pwd

security-password warning

username

security-password minimum-length

Overview This command specifies the minimum allowable password length. This value is checked against when there is a password change or a user account is created.

Syntax

```
security-password minimum-length <1-23>
```

Parameter	Description
<1-23>	Minimum password length in the range from 1 to 23.

Default The default minimum password length is `1`.

Mode Global Configuration

Example To configure the required minimum password length as `8`, use the command:

```
awplus# configure terminal
awplus(config)# security-password minimum-length 8
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password history

security-password forced-change

security-password lifetime

security-password minimum-categories

security-password reject-expired-pwd

security-password warning

username

security-password reject-expired-pwd

Overview This command specifies whether or not a user is allowed to login with an expired password. Users with expired passwords are rejected at login if this functionality is enabled. Users then have to contact the Network Administrator to change their password.

CAUTION: *Once all users' passwords are expired you are unable to login to the device again if the security-password reject-expired-pwd command has been executed. You will have to reboot the device with a default configuration file, or load an earlier software version that does not have the security password feature.*

We recommend you never have the command line "security-password reject-expired-pwd" in a default config file.

Note that when the reject-expired-pwd functionality is disabled and a user logs on with an expired password, if the forced-change feature is enabled with security-password forced-change command, a user may have to change the password during login depending on the password lifetime specified by the security-password lifetime command.

The **no security-password reject-expired-pwd** command disables the reject-expired-pwd feature.

Syntax

```
security-password reject-expired-pwd
no security-password reject-expired-pwd
```

Default The reject-expired-pwd feature is disabled by default.

Mode Global Configuration

Example To configure the system to reject users with an expired password, use the command:

```
awplus# configure terminal
awplus(config)# security-password reject-expired-pwd
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password history

security-password forced-change

security-password lifetime

security-password minimum-categories

security-password minimum-length

security-password warning

show security-password user

security-password warning

Overview This command specifies the number of days before the password expires that the user will receive a warning message specifying the remaining lifetime of the password.

Note that the warning period cannot be set unless the lifetime feature is enabled with the security-password lifetime command.

The **no security-password warning** command disables this feature.

Syntax

```
security-password warning <0-1000>
no security-password warning
```

Parameter	Description
<0-1000>	Warning period in the range from *0* to *1000* days. A value *0* disables the warning functionality and no warning message is displayed for expiring passwords. This is equivalent to the **no security-password warning** command. The warning period must be less than, or equal to, the password lifetime set with the security-password lifetime command.

Default The default warning period is `0`, which disables warning functionality.

Mode Global Configuration

Example To configure a warning period of three days, use the command:

```
awplus# configure terminal
awplus(config)# security-password warning 3
```

Validation Commands

show running-config security-password

show security-password configuration

Related Commands

security-password history

security-password forced-change

security-password lifetime

security-password minimum-categories

security-password minimum-length

security-password reject-expired-pwd

service advanced-vty

Overview This command enables the advanced-vty help feature. This allows you to use TAB completion for commands. Where multiple options are possible, the help feature displays the possible options.

The **no service advanced-vty** command disables the advanced-vty help feature.

Syntax

```
service advanced-vty
no service advanced-vty
```

Default The advanced-vty help feature is enabled by default.

Mode Global Configuration

Examples To disable the advanced-vty help feature, use the command:

```
awplus# configure terminal
awplus(config)# no service advanced-vty
```

To re-enable the advanced-vty help feature after it has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service advanced-vty
```

service password-encryption

Overview Use this command to enable password encryption. This is enabled by default. When password encryption is enabled, the device displays passwords in the running config in encrypted form instead of in plain text.

Use the **no service password-encryption** command to stop the device from displaying newly-entered passwords in encrypted form. This does not change the display of existing passwords.

NOTE: *Do not use encrypted passwords for GUI users. The GUI requires unencrypted user passwords only - not encrypted user passwords. Do not use option 8 for GUI users.*

Syntax

```
service password-encryption
no service password-encryption
```

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# service password-encryption
```

Validation Commands show running-config

Related Commands enable password

service telnet

Overview Use this command to enable the telnet server. The server is enabled by default. Enabling the telnet server starts the device listening for incoming telnet sessions on the configured port.

The server listens on port 23, unless you have changed the port by using the privilege level command.

Use the **no** variant of this command to disable the telnet server. Disabling the telnet server will stop the device listening for new incoming telnet sessions. However, existing telnet sessions will still be active.

Syntax

```
service telnet [ip|ipv6]
no service telnet [ip|ipv6]
```

Default The IPv4 and IPv6 telnet servers are enabled by default.

The configured telnet port is TCP port 23 by default.

Mode Global Configuration

Examples To enable both the IPv4 and IPv6 telnet servers, use the following commands:

```
awplus# configure terminal
awplus(config)# service telnet
```

To enable the IPv6 telnet server only, use the following commands:

```
awplus# configure terminal
awplus(config)# service telnet ipv6
```

To disable both the IPv4 and IPv6 telnet servers, use the following commands:

```
awplus# configure terminal
awplus(config)# no service telnet
```

To disable the IPv6 telnet server only, use the following commands:

```
awplus# configure terminal
awplus(config)# no service telnet ipv6
```

Related Commands clear line vty

show telnet

telnet server

service terminal-length (deleted)

Overview This command has been deleted in Software Version 5.4.5-0.1 and later.

show privilege

Overview This command displays the current user privilege level, which can be any privilege level in the range <1-15>. Privilege levels <1-6> allow limited user access (all User Exec commands), privilege levels <7-14> allow restricted user access (all User Exec commands plus Privileged Exec show commands). Privilege level 15 gives full user access to all Privileged Exec commands.

Syntax

```
show privilege
```

Mode User Exec and Privileged Exec

Usage A user can have an intermediate CLI security level set with this command for privilege levels <7-14> to access all show commands in Privileged Exec mode and all commands in User Exec mode, but no configuration commands in Privileged Exec mode.

Example To show the current privilege level of the user, use the command:

```
awplus# show privilege
```

Output Figure 3-1: Example output from the **show privilege** command

```
awplus#show privilege
Current privilege level is 15
awplus#disable
awplus>show privilege
Current privilege level is 1
```

Related Commands privilege level

show security-password configuration

Overview This command displays the configuration settings for the various security password rules.

Syntax

```
show security-password configuration
```

Mode Privileged Exec

Example To display the current security-password rule configuration settings, use the command:

```
awplus# show security-password configuration
```

Output Figure 3-2: Example output from the **show security-password configuration** command

```
Security Password Configuration
Minimum password length ..............................  8
Minimum password character categories to match .....  3
Number of previously used passwords to restrict.....  4
Password lifetime ....................................  30 day(s)
  Warning period before password expires ............  3 day(s)
Reject expired password at login .....................  Disabled
  Force changing expired password at login .........  Enabled
```

Related Commands

show running-config security-password

show security-password user

show security-password user

Overview This command displays user account and password information for all users.

Syntax

```
show security-password user
```

Mode Privileged Exec

Example To display the system users' remaining lifetime or last password change, use the command:

```
awplus# show security-password user
```

Output Figure 3-3: Example output from the **show security-password** user command

```
User account and password information

UserName          Privilege Last-PWD-Change   Remaining-lifetime
-------------------------------------------------------------------
manager           15          4625 day(s) ago   No Expiry
bob15             15             0 day(s) ago   30 days
ted7              7              0 day(s) ago   No Expiry
mike1             1              0 day(s) ago   No Expiry
```

Related Commands

show running-config security-password

show security-password configuration

show telnet

Overview This command shows the Telnet server settings.

Syntax

```
show telnet
```

Mode User Exec and Privileged Exec

Example To show the Telnet server settings, use the command:

```
awplus# show telnet
```

Output Figure 3-4: Example output from the **show telnet** command

```
Telnet Server Configuration
-------------------------------------------------------------
Telnet server               : Enabled
Protocol                    : IPv4,IPv6
Port                        : 23
```

Related Commands

clear line vty

service telnet

show users

telnet server

show users

Overview This command shows information about the users who are currently logged into the device.

Syntax

```
show users
```

Mode User Exec and Privileged Exec

Example To show the users currently connected to the device, use the command:

```
awplus# show users
```

Output Figure 3-5: Example output from the **show users** command

```
Line     User             Host(s)  Idle      Location         Priv Idletime Timeout
con 0    manager          idle     00:00:00  ttyS0            15   10       N/A
vty 0    bob              idle     00:00:03  172.16.11.3      1    0        5
```

Table 1: Parameters in the output of the **show users** command

Parameter	Description
Line	Console port user is connected to.
User	Login name of user.
Host(s)	Status of the host the user is connected to.
Idle	How long the host has been idle.
Location	URL location of user.
Priv	The privilege level in the range 1 to 15, with 15 being the highest.
Idletime	The time interval the device waits for user input from either a console or VTY connection.
Timeout	The time interval before a server is considered unreachable.

telnet

Overview Use this command to open a telnet session to a remote device.

Syntax

```
telnet {<hostname>|[ip] <ipv4-addr>|[ipv6] <ipv6-addr>}
[<port>]
```

Parameter	Description
<hostname>	The host name of the remote system.
ip	Keyword used to specify the IPv4 address or host name of a remote system.
<ipv4-addr>	An IPv4 address of the remote system.
ipv6	Keyword used to specify the IPv6 address of a remote system
<ipv6-addr>	Placeholder for an IPv6 address in the format x:x::x:x, for example, 2001:db8::8a2e:7334
<port>	Specify a TCP port number (well known ports are in the range 1-1023, registered ports are 1024-49151, and private ports are 49152-65535).

Mode User Exec and Privileged Exec

Examples To connect to TCP port 2602 on the device at 10.2.2.2, use the command:

```
awplus# telnet 10.2.2.2 2602
```

To connect to the telnet server host.example, use the command:

```
awplus# telnet host.example
```

To connect to the telnet server host.example on TCP port 100, use the command:

```
awplus# telnet host.example 100
```

telnet server

Overview This command enables the telnet server on the specified TCP port. If the server is already enabled then it will be restarted on the new port. Changing the port number does not affect the port used by existing sessions.

Syntax

```
telnet server {<1-65535>|default}
```

Parameter	Description
<1-65535>	The TCP port to listen on.
`default`	Use the default TCP port number 23.

Mode Global Configuration

Example To enable the telnet server on TCP port 2323, use the following commands:

```
awplus# configure terminal
awplus(config)# telnet server 2323
```

Related Commands show telnet

terminal length

Overview Use the **terminal length** command to specify the number of rows of output that the device will display before pausing, for the currently-active terminal only.

Use the **terminal no length** command to remove the length specified by this command. The default length will apply unless you have changed the length for some or all lines by using the length (asyn) command.

Syntax

```
terminal length <length>
terminal no length [<length>]
```

Parameter	Description
<length>	<0-512> Number of rows that the device will display on the currently-active terminal before pausing.

Mode User Exec and Privileged Exec

Examples The following example sets the number of lines to 15:

```
awplus# terminal length 15
```

The following example removes terminal length set previously:

```
awplus# terminal no length
```

Related Commands terminal resize

length (asyn)

terminal resize

Overview Use this command to automatically adjust the number of rows of output on the console, which the device will display before pausing, to the number of rows configured on the user's terminal.

Syntax

```
terminal resize
```

Mode User Exec and Privileged Exec

Usage When the user's terminal size is changed, then a remote session via SSH or TELNET adjusts the terminal size automatically. However, this cannot normally be done automatically for a serial or console port. This command automatically adjusts the terminal size for a serial or console port.

Examples The following example automatically adjusts the number of rows shown on the console:

```
awplus# terminal resize
```

Related Commands length (asyn)

terminal length

username

Overview This command creates or modifies a user to assign a privilege level and a password.

NOTE: *The default username privilege level of 1 is not shown in running-config output. Any username privilege level that has been modified from the default is shown.*

Syntax

```
username <name> privilege <0-15> [password [8] <password>]
username <name> password [8] <password>
no username <name>
```

Parameter	Description	
<name>	The login name for the user. Do not use punctuation marks such as single quotes (‘ ‘), double quotes (“ “), or colons (:) with the user login name.	
privilege	The user’s privilege level. Use the privilege levels to set the access rights for each user.	
	<0-15>	A privilege level: either 0 (no access), 1-14 (limited access) or 15 (full access). A user with privilege level 1-14 can only access higher privilege levels if an enable password has been configured for the level the user tries to access and the user enters that password. A user at privilege level 1 can access the majority of show commands. A user at privilege level 7 can access the majority of show commands including platform show commands. Privilege Level 15 (to access the Privileged Exec command mode) is required to access configuration commands as well as show commands in Privileged Exec.
password	A password that the user must enter when logging in.	
	8	Specifies that you are entering a password as a string that has already been encrypted, instead of entering a plain-text password. The running-config displays the new password as an encrypted string even if password encryption is turned off. Note that the user enters the plain-text version of the password when logging in.
	<password>	The user’s password. The password can be up to 23 characters in length and include characters from up to four categories. The password categories are: • uppercase letters: A to Z • lowercase letters: a to z • digits: 0 to 9 • special symbols: all printable ASCII characters not included in the previous three categories. The question mark ? cannot be used as it is reserved for help functionality.

Mode Global Configuration

Default The privilege level is 1 by default. Note the default is not shown in running-config output.

Usage

An intermediate CLI security level (privilege level 7 to privilege level 14) allows a CLI user access to the majority of show commands, including the platform show commands that are available at privilege level 1 to privilege level 6). Note that some show commands, such as show running-configuration and show startup-configuration, are only available at privilege level 15.

A privilege level of 0 can be set for port authentication purposes from a RADIUS server.

Examples

To create the user `bob` with a privilege level of `15`, for all show commands including show running-configuration and show startup-configuration and to access configuration commands in Privileged Exec command mode, and the password `bobs_secret`, use the commands:

```
awplus# configure terminal
awplus(config)# username bob privilege 15 password bobs_secret
```

To create a user `junior_admin` with a privilege level of `7`, for intermediate CLI security level access for most show commands, and the password `show_only`, use the commands:

```
awplus# configure terminal
awplus(config)# username junior_admin privilege 7 password
show_only
```

Related Commands

enable password

security-password minimum-categories

security-password minimum-length

4 Licensing Commands

Introduction

Overview This chapter provides an alphabetical reference for each of the License commands.

Command List

license

Overview This command activates the licensed software feature set on a standalone switch, or a stack of switches.

Use the **no** variant of this command to deactivate the licensed software feature set on a standalone switch, or a stack of switches.

For feature licenses, contact your authorized distributor or reseller. If a license key expires or is incorrect so the license key is invalid, then some software features will be unavailable.

NOTE: *See the AlliedWare Plus™ datasheet for a list of current feature licenses available by product, and the AlliedWare Plus™ How To notes for information on obtaining them. Purchase licenses from your authorized dealer or reseller.*

Only install feature licenses during scheduled maintenance for any devices in a live environment. For example, if a feature license includes EPSR, EPSR is restarted with a temporary loss of EPSR network traffic.

Syntax

```
license <label> <key>
no license <label>
```

Parameter	Description
<label>	A name for the feature license. To determine names already in use, use the show license command. This can be the default name supplied for the feature, or a renamed feature name.
<key>	The encrypted license key to enable a set of software features.

Mode Privileged Exec

Usage You can change the license label using this command to make it specific to you when you initially add a license. Once a license is added, any change to the license label first requires removal of the license before adding a license again with a new license label.

The default feature license labels are issued along with encrypted license keys by e-mail for you to apply using this command to activate features. You can change default feature license labels, but they must be 15 characters or less to be accepted with the issued keys.

For example, you may want to change the label of the premium license to “premium- license”. You can check your new license label by using the show license command.

In a stacked configuration, the **license** command will add a license to all stack members and the **no license** command will remove a license from all stack members.

You can add a license to a specified stack member after first using the remote-login command from the stack master. Adding or deleting licenses on individual

switches can cause different members of the stack to have different features enabled, which may cause the stack to fail to operate correctly. Unbalanced stack members will not form a stack. Stack members require the same feature licenses to be balanced.

If you add a feature license you will be prompted at the console that the feature needs to restart. For example, if the feature license contains a license for the EPSR protocol, then that protocol will restart. This action may result in the loss of network traffic. Only install licenses in scheduled maintenance periods for devices in a live environment.

Examples To activate the license `name1` with the key `12345678ABCDE123456789ABCDE`, use the command:

```
awplus# license name1 12345678ABCDE123456789ABCDE
```

To deactivate the license `name1`, use the command:

```
awplus# no license name1
```

Output Figure 4-1: Example of a license command entry to remove a feature license

```
awplus#no license IPv6
Stack member 1: Removal of "IPv6" will disable the following features:
 IPv6

INFO: Uninstalling license key will disable the affected modules immediately.
Would you like to continue? (y/n): y

Stack member 1 removed 1 license

1 license removed.
```

Validation Command show license

license member (deleted)

Overview This command has been deleted. Instead, use the license command to apply licenses to VCStack members.

In a stacked configuration, the license command will add a license to all stack members and the **no license** command will remove a license from all stack members.

show license

Overview This command displays information about a specific software feature license, or all enabled software feature licenses on the device.

Syntax

```
show license [feature] [<label>|index <index-number>]
```

Parameter	Description
`feature`	Only display license information for any applied feature licenses.
`<label>`	The license name to show information about. This can be used instead of the index number to identify a specific license.
`index <index-number>`	The index number of the license to show information about. This can be used instead of the license name to identify a specific license.

Mode User Exec and Privileged Exec

Usage This command will display licenses applied to a stack master only.

In a stacked configuration, use the show license member command instead if you need to display license information for a specific stack member or all stack members.

Examples To display full information about all enabled licenses, use the command:

```
awplus# show license
```

To display full information about the licenses with index number 1, use the command:

```
awplus# show license index 1
```

Output Figure 4-2: Example output from **show license**

```
awplus#show license
Board region: Global
Software Licenses
------------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : Base License
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 12-Jul-2014
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100, VCS,
                                 VRRP
```

Table 4-1: Parameters in the output of **show license**

Parameter	Description
Board region	Name of the region for the Base License features.
Index	Index identifying entry. The index is assigned automatically by the software. It is not configured.
License name	Name of the license key bundle (case-sensitive).
Customer name	Customer name.
Quantity of licenses	Quantity of licensed installations.
Type of license	Full or Trial.
License issue date	Date the license was generated.
License expiry date	Expiry date for trial license.
Features included	List of features included in the feature license.

Related Commands

license

show license brief

show license member

show license brief

Overview This command displays information about a specific software feature license, or all enabled software feature licenses on the device.

Syntax

```
show license [feature] [<label>|index <index-number>] brief
```

Parameter	Description
`feature`	Only display license information for any applied feature licenses.
`<label>`	The license name to show information about. This can be used instead of the index number to identify a specific license.
`index <index-number>`	The index number of the license to show information about. This can be used instead of the license name to identify a specific license.
`brief`	Displays a brief summary of license information.

Mode User Exec and Privileged Exec

Usage This command will display licenses applied to a stack master only.

In a stacked configuration, use the show license brief member command instead if you need to display license information for a specific stack member or all stack members.

Examples To display a brief summary of information about all feature licenses, use the command:

```
awplus# show license feature brief
```

Output Figure 4-3: Example output from **show license brief**

```
awplus#show license brief
Board region: Global
Software Licenses
-------------------------------------------------------------------------
Index License name    Quantity     Customer name
      Type            Version      Period
-------------------------------------------------------------------------
1     Base License    1            Base License
      Full                         N/A

Current enabled features for displayed licenses:
 IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100, VCS, VRRP
```

Table 4-2: Parameters in the output of **show license brief**

Parameter	Description
Board region	Name of the region for the Base License features.
Index	Index identifying entry. The index is assigned automatically by the software. It is not configured.
License name	Name of the license key bundle (case-sensitive).
Quantity	Quantity of licensed installations.
Customer name	Customer name.
Type	Full or Trial.
Period	Expiry date for trial license.
Current enabled features for displayed licenses	List of features included in the license.

Related Commands

license

show license

show license member

show license brief member

Overview Use this command to display information about either a specific software license, or all software feature licenses enabled on either a specific stack member or all stack members.

Syntax

```
show license [<label>] brief member [<1-8>|all]
```

Parameter	Description
<label>	The name of the license to show information about.
`brief`	Display a brief summary of license information.
<1-8>	The ID of the stack member to show information about.
`all`	Display information about all stack members.

Mode User Exec and Privileged Exec

Usage Use the **show license brief member all** command for brief table output of all licenses per stack member.

Examples To display a brief summary of information about all enabled licenses on stack member 2, use the command:

```
awplus# show license brief member 2
```

To display a brief summary about all enabled licenses on all stack members, use the command:

```
awplus# show license brief member all
```

To display a brief summary about the license `name1` on all stack members, use the command:

```
awplus# show license name1 brief member all
```

Output Figure 4-4: Example output from **show license brief member**

```
awplus#show license brief member 1
Board region: Global
Software Release Licenses
--------------------------------------------------------------------------
1
    Base License    1            Base License

    Full                         N/A

Current
enabled features for displayed licenses:
 IPv6Basic,
LAG-FULL, MLDSnoop, RADIUS-100, VCS, VRRP
```

Table 4-3: Parameters in the output of **show license brief member**

Parameter	Description
`Board region`	Name of the region for the Base License features.
`Index`	Index identifying entry. The index is assigned automatically by the software. It is not configured.
`License name`	Name of the license key bundle (case-sensitive).
`Quantity`	Quantity of licensed installations.
`Customer name`	Customer name.
`Type`	Full or Trial.
`Period`	Expiry date for trial license.
`Current enabled features for displayed licenses`	List of features included in the license.

Related Commands

license

show license

show license member

show license member

Overview Use this command to display information about either a specific software license, or all software feature licenses enabled on either a specific stack member or all stack members.

Syntax

```
show license [<label>] member [<1-8>|all]
```

Parameter	Description
<label>	The name of the license to show information about.
<1-8>	The ID of the stack member to show information about.
`all`	Display information about all stack members.

Mode User Exec and Privileged Exec

Usage Use the **show license member all** command to display full list output of all licenses per stack member.

Examples To display full information about all enabled licenses on all stack members, use the command:

```
awplus# show license member all
```

To display full information about all enabled licenses on stack member 2, use the command:

```
awplus# show license member 2
```

To display full information about the license `name1` on all stack members, use the command:

```
awplus# show license name1 member all
```

Output Figure 4-5: Example output from **show license member**

```
awplus#show license member all
Board region: Global
Software Feature Licenses
----------------------------------------------------------------------
Index                          : 1
License name                   : Base License
Customer name                  : Base License
Quantity of licenses           : 1
Type of license                : Full
License issue date             : 12-Jul-2014
License expiry date            : N/A
Features included              : IPv6Basic, LAG-FULL, MLDSnoop, RADIUS-100, VCS,
                                 VRRP

Index                          : 2
License name                   : PIM Trial
Customer name                  : PIM Trial
Quantity of licenses           : 10
Type of license                : 30 day trial
License issue date             : 12-Jul-2014
License expiry date            : 12-Jul-2014
Features included              : PIM PIM-100
```

Table 4-4: Parameters in the output of **show license member**

Parameter	Description
Board region	Name of the region for the Base License features.
Index	Index identifying entry. The index is assigned automatically by the software. It is not configured.
License name	Name of the license key bundle (case-sensitive).
Customer name	Customer name.
Quantity of licenses	Quantity of licensed installations.
Type of license	Full or Trial.
License issue date	Date the license was generated.
License expiry date	Expiry date for trial license.
Features included	List of features included in the license.

Related Commands

license

show license

show license brief member

5 GUI Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure the GUI. For more information, see the Getting Started with Alliedware Plus

Command List

gui-timeout

Overview Use this command to configure an idle timeout period for a GUI session. The time can be set in minutes and/or seconds.

Use the **no** variant of this command to disable the GUI session idle timeout.

Syntax

```
gui-timeout {<minutes>}|[<seconds>]
no gui-timeout
```

Parameter	Description
<minutes>	Specifies the idle time in minutes from 0 through 35791
<seconds>	Specifies the idle time in seconds from 0 through 2147483

Default Disabled

Mode Configuration

Usage The GUI uses the configured timeout period (set in either minutes and/or seconds) to determine when a GUI session should be closed. Once the GUI timeout has expired, you will need to login to reactivate your session.

To enter seconds only, enter 0 for minutes, followed by a space, and then enter the seconds.

If the GUI timeout is disabled, a GUI session will remain active until you terminate it, no idle time will be configured. The same timeout period will apply to all GUI sessions logged into a specific stand-alone device or stack.

Examples Use this command to configure the GUI timeout period for 3 minutes and 30 seconds for a GUI session.

```
awplus# gui-timeout 3 30
```

Use this command to configure the GUI timeout period for 0 minutes and 61 seconds for a GUI session.

```
awplus# gui-timeout 0 61
```

Use this command to disable the GUI timeout period.

```
awplus# no gui-timeout
```

Output Figure 5-1: Example output from **gui-timeout**

```
awplus#configure terminal
awplus(config)#gui-timeout 3 30
The new gui-timeout settings [3 min 30 sec] will apply to new sessions only
```

Related Commands show running-config

service http

Overview Use this command to enable the HTTP (Hypertext Transfer Protocol) service. This service, which is enabled by default, is required to support the AlliedWare Plus™ GUI Java applet on a Java enabled browser.

Use the **no** variant of this command to disable the HTTP feature.

Syntax

```
service http
no service http
```

Default Enabled

Mode Global Configuration

Validation Commands show running-config

show http

Overview This command shows the HTTP server settings.

Syntax

```
show http
```

Mode User Exec and Privileged Exec

Example To show the HTTP server settings, use the command:

```
awplus# show http
```

Output Figure 5-2: Example output from the **show http** command

```
awplus#show http
HTTP Server Configuration
-----------------------------------------------------------
HTTP server                  : Enabled
Port                              : 80
Web GUI Information
-----------------------------------------------------------
GUI file in use                : webguiGUI
version:                       : 3.1
```

Related Commands

clear line vty

service http

6 System Configuration and Monitoring Commands

Introduction

Overview This chapter provides an alphabetical reference of commands for configuring and monitoring the system.

Command List

banner exec

Overview This command configures the User Exec mode banner that is displayed on the console after you login. The **banner exec default** command restores the User Exec banner to the default banner. Use the **no banner exec** command to disable the User Exec banner and remove the default User Exec banner.

Syntax

```
banner exec <banner-text>
banner exec default
no banner exec
```

Default By default, the AlliedWare Plus™ version and build date is displayed at console login, such as:

```
AlliedWare Plus (TM) 5.4.6-0 03/31/14 00:44:25
```

Mode Global Configuration

Examples To configure a User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal

awplus(config)#banner exec enable to move to Priv Exec mode

awplus(config)#exit

awplus#exit
awplus login: manager

Password:

enable to move to Priv Exec mode

awplus>
```

To restore the default User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal

awplus(config)#banner exec default

awplus(config)#exit

awplus#exit
awplus login: manager

Password:

AlliedWare
Plus (TM) 5.4.6-0 03/31/14
13:03:59
awplus>
```

To remove the User Exec mode banner after login, enter the following commands:

```
awplus#configure terminal

awplus(config)#no banner exec

awplus(config)#exit

awplus#exit

awplus login: manager

Password:

awplus>
```

Related Commands

banner login (system)

banner motd

banner login (system)

Overview This command configures the login banner that is displayed on the console when you login. The login banner is displayed on all connected terminals. The login banner is displayed after the MOTD (Message-of-the-Day) banner and before the login username and password prompts.

Use the **no banner login** command to disable the login banner.

Syntax

```
banner login
no banner login
```

Default By default, no login banner is displayed at console login.

Mode Global Configuration

Examples To configure a login banner to be displayed when you login, enter the following commands:

```
awplus#configure terminal

awplus(config)#banner login

Type CNTL/D to finish.

authorised users only

awplus(config)#exit

awplus#exit

authorised users only

awplus login: manager

Password:

AlliedWare
Plus (TM) 5.4.6-0 03/31/14
13:03:59
awplus>
```

To remove the login banner, enter the following commands:

```
awplus#configure terminal

awplus(config)#no banner login

awplus(config)#exit

awplus#exit

awplus login: manager

Password:

awplus>
```

Related Commands

banner exec

banner motd

banner motd

Overview Use this command to create or edit the text MotD (Message-of-the-Day) banner displayed before login. The MotD banner is displayed on all connected terminals. The MotD banner is useful for sending messages that affect all network users, for example, any imminent system shutdowns.

Use the **no** variant of this command to delete the MotD banner.

Syntax

```
banner motd <motd-text>
no banner motd
```

Parameter	Description
<motd-text>	The text to appear in the Message of the Day banner.

Default By default, the device displays the AlliedWare Plus™ OS version and build date when you login.

Mode Global Configuration

Examples To configure a MotD banner to be displayed when you log in, enter the following commands:

```
awplus>enable

awplus#configure terminal

awplus(config)#banner motd system shutdown at 6pm

awplus(config)#exit

awplus#exit

system shutdown at 6pm


awplus login: manager

Password:

AlliedWare
Plus (TM) 5.4.6-0 03/31/14
13:03:59
```

To delete the login banner, enter the following commands:

```
awplus>enable

awplus#configure terminal

awplus(config)#no banner motd

awplus(config)#exit

awplus#exit

awplus login: manager

Password:

AlliedWare
Plus (TM) 5.4.6-0 03/31/14
13:03:59
awplus>
```

Related Commands

banner exec

banner login (system)

clock set

Overview This command sets the time and date for the system clock.

Syntax

```
clock set <hh:mm:ss> <day> <month> <year>
```

Parameter	Description
<hh:mm:ss>	Local time in 24-hour format
<day>	Day of the current month <1-31>
<month>	The first three letters of the current month.
<year>	Current year <2000-2035>

Mode Privileged Exec

Usage Configure the timezone before setting the local time. Otherwise, when you change the timezone, the device applies the new offset to the local time.

NOTE: *If Network Time Protocol (NTP) is enabled, then you cannot change the time or date using this command. NTP maintains the clock automatically using an external time source. If you wish to manually alter the time or date, you must first disable NTP.*

Example To set the time and date on your system to 2pm on the 2nd of April 2007, use the command:

```
awplus# clock set 14:00:00 2 apr 2007
```

Related Commands clock timezone

clock summer-time date

Overview This command defines the start and end of summertime for a specific year only, and specifies summertime's offset value to Standard Time for that year.

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates and recurring dates (set with the clock summer-time recurring command).

By default, the device has no summertime definitions set.

Syntax

```
clock summer-time <timezone-name> date <start-day>
<start-month> <start-year> <start-time> <end-day>
<end-month> <end-year> <end-time> <1-180>
```

```
no clock summer-time
```

Parameter	Description
<timezone-name>	A description of the summertime zone, up to 6 characters long.
date	Specifies that this is a date-based summertime setting for just the specified year.
<start-day>	Day that the summertime starts, in the range 1-31.
<start-month>	First three letters of the name of the month that the summertime starts.
<start-year>	Year that summertime starts, in the range 2000-2035.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-day>	Day that summertime ends, in the range 1-31.
<end-month>	First three letters of the name of the month that the summertime ends.
<end-year>	Year that summertime ends, in the range 2000-2035.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with the summertime set to begin on the 1st October 2007 and end on the 18th of March 2008:

```
awplus(config)# clock summer-time NZDT date 1 oct 2:00 2007 18
mar 2:00 2008 60
```

To remove any summertime settings on the system, use the command:

```
awplus(config)# no clock summer-time
```

Related Commands

clock summer-time recurring

clock timezone

clock summer-time recurring

Overview This command defines the start and end of summertime for every year, and specifies summertime's offset value to Standard Time.

The **no** variant of this command removes the device's summertime setting. This clears both specific summertime dates (set with the clock summer-time date command) and recurring dates.

By default, the device has no summertime definitions set.

Syntax

```
clock summer-time <timezone-name> recurring <start-week>
<start-day> <start-month> <start-time> <end-week> <end-day>
<end-month>  <end-time> <1-180>
```

```
no clock summer-time
```

Parameter	Description
<timezone-name>	A description of the summertime zone, up to 6 characters long.
`recurring`	Specifies that this summertime setting applies every year from now on.
<start-week>	Week of the month when summertime starts, in the range 1-5. The value 5 indicates the last week that has the specified day in it for the specified month. For example, to start summertime on the last Sunday of the month, enter 5 for <*start-week*> and sun for <*start-day*>.
<start-day>	Day of the week when summertime starts. Valid values are mon, tue, wed, thu, fri, sat or sun.
<start-month>	First three letters of the name of the month that summertime starts.
<start-time>	Time of the day that summertime starts, in the 24-hour time format HH:MM.
<end-week>	Week of the month when summertime ends, in the range 1-5. The value 5 indicates the last week that has the specified day in it for the specified month. For example, to end summertime on the last Sunday of the month, enter 5 for <*end-week*> and sun for <*end-day*>.
<end-day>	Day of the week when summertime ends. Valid values are mon, tue, wed, thu, fri, sat or sun.
<end-month>	First three letters of the name of the month that summertime ends.
<end-time>	Time of the day that summertime ends, in the 24-hour time format HH:MM.
<1-180>	The offset in minutes.

Mode Global Configuration

Examples To set a summertime definition for New Zealand using NZST (UTC+12:00) as the standard time, and NZDT (UTC+13:00) as summertime, with summertime set to start on the 1st Sunday in October, and end on the 3rd Sunday in March, use the command:

```
awplus(config)# clock summer-time NZDT recurring 1 sun oct 2:00
3 sun mar 2:00 60
```

To remove any summertime settings on the system, use the command:

```
awplus(config)# no clock summer-time
```

Related Commands clock summer-time date

clock timezone

clock timezone

Overview This command defines the device's clock timezone. The timezone is set as a offset to the UTC.

The **no** variant of this command resets the system time to UTC.

By default, the system time is set to UTC.

Syntax

```
clock timezone <timezone-name> {minus|plus}
[<0-13>|<0-12>:<00-59>]
```

```
no clock timezone
```

Parameter	Description
<timezone-name>	A description of the timezone, up to 6 characters long.
minus orplus	The direction of offset from UTC. The **minus** option indicates that the timezone is behind UTC. The **plus** option indicates that the timezone is ahead of UTC.
<0-13>	The offset in hours or from UTC.
<0-12>:<00-59>	The offset in hours or from UTC.

Mode Global Configuration

Usage Configure the timezone before setting the local time. Otherwise, when you change the timezone, the device applies the new offset to the local time.

Examples To set the timezone to New Zealand Standard Time with an offset from UTC of +12 hours, use the command:

```
awplus(config)# clock timezone NZST plus 12
```

To set the timezone to Indian Standard Time with an offset from UTC of +5:30 hours, use the command:

```
awplus(config)# clock timezone IST plus 5:30
```

To set the timezone back to UTC with no offsets, use the command:

```
awplus(config)# no clock timezone
```

Related Commands

clock set

clock summer-time date

clock summer-time recurring

continuous-reboot-prevention

Overview Use this command to enable and to configure the continuous reboot prevention feature. Continuous reboot prevention allows the user to configure the time period during which reboot events are counted, the maximum number of times the switch can reboot within the specified time period, referred to as the threshold, and the action to take if the threshold is exceeded.

Use the **no** variant of this command to disable the continuous reboot prevention feature or to return the **period**, **threshold** and **action** parameters to the defaults.

Syntax

```
continuous-reboot-prevention enable
continuous-reboot-prevention [period <0-604800>] [threshold <1-10>] [action [linkdown|logonly|stopreboot]]
no continuous-reboot-prevention enable
no continuous-reboot-prevention [period] [threshold] [action]}
```

Parameter	Description	
`enable`	Enable the continuous reboot prevention feature.	
`period`	Set the period of time in which reboot events are counted.	
	<0-604800>	Period value in seconds. The default is 600.
`threshold`	Set the maximum number of reboot events allowed in the specified period.	
	<1-10>	Threshold value. The default is 1.
`action`	Set the action taken if the threshold is exceeded.	
	`linkdown`	Reboot procedure continues and all switch ports and stack ports stay link-down. The reboot event is logged. This is the default action.
	`logonly`	Reboot procedure continues normally and the reboot event is logged.
	`stopreboot`	Reboot procedure stops until the user enters the key "c" via the CLI. Normal reboot procedure then continues and the reboot event is logged.

Default Continuous reboot prevention is disabled by default. The default `period` value is `600`, the default `threshold` value is `1` and the default `action` is `linkdown`.

Mode Global Configuration

Usage Note that user initiated reboots via the CLI, and software version auto-synchronization reboots, are not counted toward the threshold value.

Examples

To enable continuous reboot prevention, use the commands:

```
awplus# configure terminal
awplus(config)# continuous-reboot-prevention enable
```

To set the `period` to `500` and `action` to `stopreboot`, use the commands:

```
awplus# configure terminal
awplus(config)# continuous-reboot-prevention period 500 action
stopreboot
```

To return the `period` and `action` to the defaults and keep the continuous reboot prevention feature enabled, use the commands:

```
awplus# configure terminal
awplus(config)# no continuous-reboot-prevention period action
```

To disable continuous reboot prevention, use the commands:

```
awplus# configure terminal
awplus(config)# no continuous-reboot-prevention enable
```

Related Commands

show continuous-reboot-prevention

show reboot history

show tech-support

ecofriendly led

Overview Use this command to enable the eco-friendly LED (Light Emitting Diode) feature, which turns off power to the port LEDs, including the stack port status LEDs. Power to the system status and stack management LEDs is not disabled.

Use the **no** variant of this command to disable the eco-friendly LED feature.

Syntax

```
ecofriendly led
no ecofriendly led
```

Default The eco-friendly LED feature is disabled by default.

Mode Global Configuration

Usage When the eco-friendly LED feature is enabled, a change in port status will not affect the display of the associated LED. When the eco-friendly LED feature is disabled and power is returned to port LEDs, the LEDs will correctly show the current state of the ports.

In a stack environment, enabling the eco-friendly LED feature on the stack master will apply the feature to every member of the stack.

For an example of how to configure a trigger to turn off power to port LEDs, see the Triggers Feature Overview and Configuration Guide.

Examples To enable the eco-friendly LED feature which turns off power to all port LEDs, use the following commands:

```
awplus# configure terminal
awplus(config)# ecofriendly led
```

To disable the eco-friendly LED feature, use the following command:

```
awplus# configure terminal
awplus(config)# no ecofriendly led
```

Related Commands ecofriendly lpi

show ecofriendly

ecofriendly lpi

Use this command to conserve power by enabling the eco-friendly LPI (Low Power Idle) feature. This feature reduces the power supplied to the ports by the switch whenever the ports are idle and are connected to IEEE 802.3az Energy Efficient Ethernet compliant host devices.

LPI is a feature of the IEEE 802.3az Energy Efficient Ethernet (EEE) standard. LPI lowers power consumption of switch ports during periods of low link utilization when connected to IEEE 802.3az compliant host devices. If no data is sent then the switch port can enter a sleep state, called Low Power Idle (LPI), to conserve power used by the switch.

Use the **no** variant of this command to disable the eco-friendly LPI feature.

Syntax

```
ecofriendly lpi
no ecofriendly lpi
```

Default The eco-friendly LPI feature is disabled by default.

Mode Interface Configuration for a switch port, or Interface Configuration for a range of switch ports.

Usage For an example of how to configure a trigger to enable the eco-friendly LPI feature, see the Triggers Feature Overview and Configuration Guide.

All ports configured for LPI must support LPI in hardware and must be configured to auto negotiate by default or by using the speed and duplex commands as needed.

Examples To enable the eco-friendly LPI feature on a switch port, port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# ecofriendly lpi
```

To enable the eco-friendly LPI feature on a range of switch ports, port1.0.2-port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# ecofriendly lpi
```

To disable the eco-friendly feature on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no ecofriendly lpi
```

To disable the eco-friendly feature on a range of switch ports, port1.0.2-port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# no ecofriendly lpi
```

Related Commands

duplex

ecofriendly led

show ecofriendly

show interface

speed

findme

Overview Use this command to physically locate a specific device from a group of similar devices. Activating the command causes a selected number of port LEDs to alternately flash green then amber (if that device has amber LEDs) at a rate of 1 Hz.

Use the **no** variant of this command to deactivate the Find Me feature prior to the timeout expiring.

Syntax

```
findme [interface <port-list>|member <stack-ID>] [timeout <duration>]
no findme
```

Parameter	Description
<port-list>	The ports to flash. The port list can be: • a switch port, e.g. `port1.0.4` • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.4` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.5-1.0.6`.
<stack-ID>	Stack member number, from 1 to 8.
<duration>	Specify the duration in seconds within the range of 5-3600 seconds.

Default By default all port LEDs flash for 60 seconds.

Mode Privileged Exec

Usage Running the **findme** command causes the device's port LEDs to flash. An optional **timeout** parameter specifies the flash behavior duration. Normal LED behavior is restored automatically after either the default time, or a specified time has elapsed, or a **no findme** command is used. You can specify which interface or interfaces are flashed with the optional **interface** parameter.

You can specify a particular stack member with the optional **member** parameter. All available interfaces are flashed by default.

NOTE: *The **interface** and **member** parameters are mutually exclusive.*

Example To activate the Find Me feature for the default duration (60 seconds) on all ports, use the following command:

```
awplus# findme
```

To activate the Find Me feature for 120 seconds on all ports, use the following command:

```
awplus# findme timeout 120
```

To activate the Find Me feature for the default duration (60 seconds) on switch port interfaces `port1.0.2` through `port1.0.4`, use the following command:

```
awplus# findme interface port1.0.2-1.0.4
```

In the example above, ports 2 to 4 will flash 4 times and then all ports will flash twice. Each alternate flash will be amber (if that device has amber LEDs). This pattern will repeat until **timeout** (default or set) or **no findme** commands are used.

To deactivate the Find Me feature, use the following command:

```
awplus# no findme
```

To activate the Find Me feature for the default duration on stack member 2, use the following command:

```
awplus# findme member 2
```

In the example above, all ports on member 2 will flash 4 times and then all ports in the stack will flash twice. Each alternate flash will be amber (if that device has amber LEDs). This pattern will repeat until the **timeout** (default or set) expires or the **no findme** commands is used.

findme trigger

Overview When this command is enabled, the LED flashing functionality of the **find-me** command is applied whenever any or all of the selected parameter conditions is detected.

Use the **no** variant to remove the findme trigger function for the selected parameter.

Syntax

```
findme trigger {all|loopprot|thrash-limit|qsp}
no findme trigger {all|loopprot|thrash-limit|qsp}
```

Parameter	Description
`all`	Enable the find-me function whenever any of the listed parameter conditions is detected
`loopprot`	Enable the findme function whenever the loop protection condition is detected.
`thrash-limit`	Enable the findme function whenever the thrash-limiting condition is detected.
`qsp`	Enable the findme function whenever the QoS Storm Protection condition is detected.

Default The findme trigger function is disabled.

Mode Global config

Example To enable action LED flashing for the loop protection function:

```
awplus# findme trigger loopprot
```

Related Commands

findme

loop-protection loop-detect

storm-protection

hostname

Overview This command sets the name applied to the device as shown at the prompt. The hostname is:

- displayed in the output of the show system command
- displayed in the CLI prompt so you know which device you are configuring
- stored in the MIB object sysName

On a stack, after the stack master is elected, the master will have a host name: `awplus` by default, and this also becomes the name of the stack. Individual stack members (excluding the master) will have a host name that is the stack name hyphenated with a numeric suffix. For example, `awplus-1`, `awplus-2` and so on.

The hostname command can then be used to change the stack name and the stack master's host name. For example, for the hostname `Lab` the stack master's host name will be `Lab` and the other stack members will have host names `Lab-1`, `Lab-2` and so on.

In case of stack master fail-over, or stack split, the new stack will use the previous stack name as its host name and the stack name, unless it is changed by executing the hostname command on the new stack master.

Use the **no** variant of this command to revert the hostname setting to its default (`awplus`).

Syntax

```
hostname <hostname>
no hostname [<hostname>]
```

Parameter	Description
<hostname>	Specifies the name given to a specific device. Also referred to as the Node Name in AMF output screens.

Default `awplus`

Mode Global Configuration

Usage The name must also follow the rules for ARPANET host names. The name must start with a letter, end with a letter or digit, and use only letters, digits, and hyphens. Refer to RFC 1035.

NOTE: *Within an AMF network, any device without a hostname applied will automatically be assigned a name based on its MAC address.*

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices and accordingly apply an appropriate hostname to each device.

Example To set the system name to `HQ-Sales`, use the command:

```
awplus# configure terminal
awplus(config)# hostname HQ-Sales
```

This changes the prompt to:

```
HQ-Sales(config)#
```

To revert to the default hostname `awplus`, use the command:

```
HQ-Sales(config)# no hostname
```

This changes the prompt to:

```
awplus(config)#
```

NOTE: *When AMF is configured, running the* ***no hostname*** *command will apply a hostname that is based on the MAC address of the device node, for example,* ***node_0000_5e00_5301****.*

Related Commands show system

max-fib-routes

Overview This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds. The operation of these parameters is explained in the Parameter / Description table shown below.

NOTE: *For static routes use the max-static-routes command.*

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

Syntax

```
max-fib-routes <1-4294967294> [<1-100>|warning-only]
no max-fib-routes
```

Parameter	Description
`max-fib-routes`	This is a the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.
<1-4294967294>	The allowable configurable range for setting the maximum number of FIB-routes.
<1-100>	This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached.
`warning-only`	This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.

Default The default number of fib routes is the maximum number of fib routes (4294967294).

Mode Global Configuration

Examples To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```

max-static-routes

Overview Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

NOTE: *For FIB routes use the max-fib-routes command.*

Use the **no** variant of this command to set the maximum number of static routes to the default of 1000 static routes.

Syntax

```
max-static-routes <1-1000>
no max-static-routes
```

Default The default number of static routes is the maximum number of static routes (1000).

Mode Global Configuration

Example To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

NOTE: *Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.*

Related Commands max-fib-routes

no debug all

Overview This command disables the debugging facility for all features on your device. This stops the device from generating any diagnostic debugging messages.

The debugging facility is disabled by default.

Syntax

```
no debug all [ipv6|dot1x|nsm]
```

Parameter	Description
`dot1x`	Turns off all debugging for IEEE 802.1X port-based network access-control.
`ipv6`	Turns off all debugging for IPv6 (Internet Protocol version 6).
`nsm`	Turns off all debugging for the NSM (Network Services Module).

Mode Global Configuration and Privileged Exec

Example To disable debugging for all features, use the command:

```
awplus# no debug all
```

To disable all 802.1X debugging, use the command:

```
awplus# no debug all dot1x
```

To disable all IPv6 debugging, use the command:

```
awplus# no debug all ipv6
```

To disable all NSM debugging, use the command:

```
awplus# no debug all nsm
```

Related Commands undebug all

reboot

Overview This command halts the device and performs a cold restart (also known as reload). It displays a confirmation request before restarting.

You can reboot a stand-alone device, a stack, or a specified stack member.

Syntax

```
reboot <stack-ID>
reload <stack-ID>
reboot
reload
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.

Mode Privileged Exec

Usage The **reboot** and **reload** commands perform the same action.

When restarting the whole stack, you can either use this **reboot** command to reboot all stack members immediately, or to minimize downtime, reboot the stack members in a rolling sequence by using the reboot rolling command.

Examples To restart the device, use the command:

To restart the stand-alone device, use the command:

```
awplus# reboot
reboot system? (y/n): y
```

To restart all devices in the stack, use the command:

```
awplus# reboot
Are you sure you want to reboot the whole
stack? (y/n): y
```

To restart stack member 2, use the command:

```
awplus# reboot stack-member 2
reboot stack-member 2 system? (y/n): y
```

If the specified stack member ID does not exist in the current stack, the command is rejected.

Related Commands

reboot rolling

reload rolling

reload

Overview This command performs the same function as the reboot command.

show clock

Overview This command displays the system's current configured local time and date. It also displays other clock related information such as timezone and summertime configuration.

Syntax

```
show clock
```

Mode User Exec and Privileged Exec

Example To display the system's current local time, use the command:

```
awplus# show clock
```

Output Figure 6-1: Example output from the **show clock** command for a device using New Zealand time

```
Local Time: Mon,  6 Aug 2007 13:56:06 +1200
UTC Time:   Mon,  6 Aug 2007 01:56:06 +0000
Timezone: NZST
Timezone Offset: +12:00
Summer time zone: NZDT
Summer time starts: Last Sunday in September at 02:00:00
Summer time ends: First Sunday in April at 02:00:00
Summer time offset: 60 mins
Summer time recurring: Yes
```

Table 1: Parameters in the output of the **show clock** command

Parameter	Description
`Local Time`	Current local time.
`UTC Time`	Current UTC time.
`Timezone`	The current configured timezone name.
`Timezone Offset`	Number of hours offset to UTC.
`Summer time zone`	The current configured summertime zone name.
`Summer time starts`	Date and time set as the start of summer time.
`Summer time ends`	Date and time set as the end of summer time.
`Summer time offset`	Number of minutes that summer time is offset from the system's timezone.
`Summer time recurring`	Whether the device will apply the summer time settings every year or only once.

Related Commands

clock set

clock summer-time date

clock summer-time recurring

clock timezone

show continuous-reboot-prevention

Overview This command displays the current continuous reboot prevention configuration.

Syntax

```
show continuous-reboot-prevention
```

Mode User Exec and Privileged Exec

Examples To show the current continuous reboot prevention configuration, use the command:

```
awplus# show continuous-reboot-prevention
```

Output Figure 6-2: Example output from the **show continuous-reboot-prevention** command

```
-----------------------------------------
Continuous reboot prevention
-----------------------------------------
status=disabled
period=600
threshold=1
action=linkdown
-----------------------------------------
```

Related Commands

continuous-reboot-prevention

show reboot history

show cpu

Overview This command displays a list of running processes with their CPU utilization.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show cpu [<stack-ID>] [sort {thrds|pri|sleep|runtime}]
```

Parameter	Description	
<stack-ID>	Stack member number, from 1 to 8.	
sort	Changes the sorting order using the following fields. If you do not specify a field, then the list is sorted by percentage CPU utilization.	
	thrds	Sort by the number of threads.
	pri	Sort by the process priority.
	sleep	Sort by the average time sleeping.
	runtime	Sort by the runtime of the process.

Mode User Exec and Privileged Exec

Usage Entering this command on the stack master will display the information for all the stack members. A stack member heading will distinguish the different information for every stack member device.

Examples To show the CPU utilization of current processes, sorting them by the number of threads the processes are using, use the command:

```
awplus# show cpu sort thrds
```

Note that in a stack environment, executing this command on the stack master will show CPU utilization for all stack members.

To show CPU utilization for a specific stack member (in this case stack member 2), use the following command:

```
awplus# show cpu 2
```

Output Figure 6-3: Example output from the **show cpu** command

```
Stack
member 2:

CPU averages:
 1 second: 12%, 20 seconds: 2%, 60 seconds: 2%
System load averages:
 1 minute: 0.03, 5 minutes: 0.02, 15 minutes: 0.00
Current CPU load:
 userspace: 6%, kernel: 4%, interrupts: 1% iowaits: 0%

user processes
==============
  pid namethrds  cpu%   pri state sleep% runtime
 1544 hostd         1   2.8    20   run      0   120
 1166 exfx         17   1.8    20 sleep      0  3846
 1198 stackd        1   0.9    20 sleep      0   459
 1284 aisexec      44   0.9    -2 sleep      0  2606
    1 init          1   0.0    20 sleep      0   120
 9772 sh            1   0.0    20 sleep      0     0
 9773 corerotate    1   0.0    20 sleep      0     0
  853 syslog-ng     1   0.0    20 sleep      0   356
  859 klogd         1   0.0    20 sleep      0     1
  910 inetd         1   0.0    20 sleep      0     3
  920 portmap       1   0.0    20 sleep      0     0
  931 crond         1   0.0    20 sleep      0     1
 1090 openhpid     11   0.0    20 sleep      0   233
 1111 hpilogd      1   0.0    20 sleep      0     0
 1240 hsl          1   0.0    20 sleep      0    79
 1453 authd        1   0.0    20 sleep      0    85
 1497 cntrd        1   0.0    20 sleep      0     2
 1520 epsrd        1   0.0    20 sleep      0    56
 1571 imi          1   0.0    20 sleep      0   275
 1594 irdpd        1   0.0    20 sleep      0    23
 1617 lacpd        1   0.0    20 sleep      0    87
 1638 mstpd        1   0.0    20 sleep      0    75
 1662 nsm          1   0.0    20 sleep      0   163
 1685 ospfd        1   0.0    20 sleep      0    35
 1708 pdmd         1   0.0    20 sleep      0    23
 1729 pimd         1   0.0    20 sleep      0    32
 1751 ripd         1   0.0    20 sleep      0    33
 1775 ripngd       1   0.0    20 sleep      0    25
 1797 rmond        1   0.0    20 sleep      0    64
 1963 ntpd         1   0.0    20 sleep      0    15

...
```

Table 2: Parameters in the output of the **show cpu** command

Parameter	Description
`Stack member`	Stack member number.
`CPU averages`	Average CPU utilization for the periods stated.
`System load averages`	The average number of processes waiting for CPU time for the periods stated.
`Current CPU load`	Current CPU utilization specified by load types.
`pid`	Identifier number of the process.
`name`	A shortened name for the process
`thrds`	Number of threads in the process.
`cpu%`	Percentage of CPU utilization that this process is consuming.
`pri`	Process priority state.
`state`	Process state; one of “run”, “sleep”, “zombie”, and “dead”.
`sleep%`	Percentage of time that the process is in the sleep state.
`runtime`	The time that the process has been running for, measured in jiffies. A jiffy is the duration of one tick of the system timer interrupt.

Related Commands

show memory

show memory allocations

show memory history

show memory pools

show process

show cpu history

Overview This command prints a graph showing the historical CPU utilization.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show [<stack-ID>] cpu history
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.

Mode User Exec and Privileged Exec

Usage This command's output displays three graphs of the percentage CPU utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

If this command is entered on the stack master, it will print graphs for all the stack members. A stack member heading will be displayed to distinguish the different graphs for every stack member.

Examples To display a graph showing the historical CPU utilization of the device, use the command:

```
awplus# show cpu history
```

To display the CPU utilization history graph for stack member 2, use the command:

```
awplus# show 2 cpu history
```

where 2 is the node id of the stack member.

Output Figure 6-4: Example output from the **show cpu history** command

```
Per second CPU load history

100
 90
 80
 70
 60
 50
 40
 30
 20
 10 ************************************************************
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                 Newest
        CPU load% per second (last 60 seconds)
              * = average CPU load%


Per minute CPU load history

100        *+
 90        +
 80
 70
 60
 50
 40
 30
 20                      +                 +
 10         ************************************************
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                 Newest
        CPU load% per minute (last 60 minutes)
              * = average CPU load%, + = maximum


Per (30) minute CPU load history

100                                                          +
 90
 80
 70
 60
 50
 40
 30
 20
 10             **
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                 Newest
        CPU load% per 30 minutes (last 60 values / 30 hours)
              * = average, - = minimum, + = maximum
```

Related Commands

show memory

show memory allocations

show memory pools

show process

show debugging

Overview This command displays information for all debugging options.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging
```

Default This command runs all the **show debugging** commands in alphabetical order.

Mode User Exec and Privileged Exec

Usage This command displays all debugging information, similar to the way the show tech-support command displays all show output for use by Allied Telesis authorized service personnel only.

Example To display all debugging information, use the command:

```
awplus# show debugging
```

Output Figure 6-5: Example output from the **show debugging** command

```
awplus#show debugging
AAA debugging status:
  Authentication debugging is off
  Accounting debugging is off

% DHCP Snooping service is disabled

802.1X debugging status:

EPSR debugging status:
 EPSR Info debugging is off
 EPSR Message debugging is off
 EPSR Packet debugging is off
 EPSR State debugging is off

IGMP Debugging status:
  IGMP Decoder debugging is off
  IGMP Encoder debugging is off
...
```

show ecofriendly

Overview This command displays the switch's eco-friendly configuration status. The ecofriendly led and ecofriendly lpi configuration status are shown in the show ecofriendly output.

Syntax

```
show ecofriendly
```

Mode Privileged Exec and Global Configuration

Example To display the switch's eco-friendly configuration status, use the following command:

```
awplus# show ecofriendly
```

Output Figure 6-6: Example output from the **show ecofriendly** command

```
awplus#show ecofriendly
Front panel port LEDs          normal
Energy efficient ethernet
Port          Name             Configured  Status
port1.0.1     Port 1           lpi         lpi
port1.0.2                      lpi         lpi
port1.0.3                      lpi         lpi
port1.0.4                      off         off
port1.0.5                      lpi         off
port1.0.6     Port 6           off         off
port1.0.7                      off         -
port1.0.8                      off         -
port1.0.9                      off         -
port1.0.10                     off         -
...
```

Table 3: Parameters in the output of the **show ecofriendly** command

Parameter	Description
`normal`	The eco-friendly LED feature is disabled and port LEDs show the current state of the ports. This is the default setting.
`off`	The eco-friendly LED feature is enabled and power to the port LEDs is disabled.
`normal (configuration overridden by eco button)`	The eco-friendly LED feature has been disabled with the eco-switch button, overriding the configuration set with the ecofriendly led command. The port LEDs show the current state of the ports.

Table 3: Parameters in the output of the **show ecofriendly** command (cont.)

Parameter	Description
`off (configuration overridden by eco button)`	The eco-friendly LED feature has been enabled with the eco-switch button, overriding the configuration set with the ecofriendly led command. Power to the port LEDs is disabled.
`Port`	Displays the port number as assigned by the switch.
`Name`	Displays the port name if a name is configured for a port number.
`Configured`	The eco-friendly LPI feature is configured on the port. Either LPI or off is displayed.
`Status`	The eco-friendly LPI feature is active on the port. Either LPI or off is displayed. Ports that are not running show a dash (-).

Related Commands

ecofriendly led

ecofriendly lpi

show interface memory

Overview This command displays the shared memory used by either all interfaces, or the specified interface or interfaces. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface memory
show interface <port-list> memory
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.4`) a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Mode User Exec and Privileged Exec

Example To display the shared memory used by all interfaces, use the command:

```
awplus# show interface memory
```

To display the shared memory used by port1.0.1 and port1.0.5 to port1.0.6, use the command:

```
awplus# show interface port1.0.1,port1.0.5-1.0.6 memory
```

Output Figure 6-7: Example output from the **show interface <port-list> memory** command

```
awplus#show interface port1.0.1,port1.0.5-1.0.6 memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    393228       512            1
port1.0.5    491535       512            1
port1.0.6    557073       512            1
```

Figure 6-8: Example output from the **show interface memory** command

```
awplus#show interface memory
Vlan blocking state shared memory usage
---------------------------------------------
Interface    shmid        Bytes Used     nattch     Status
port1.0.1    393228       512            1
port1.0.2    458766       512            1
port1.0.3    360459       512            1
port1.0.4    524304       512            1
port1.0.5    491535       512            1
port1.0.6    557073       512            1
port1.0.7    327690       512            1
port1.0.8    655380       512            1
port1.0.9    622611       512            1
...
port1.0.21   950301       512            1
port1.0.22   1048608      512            1
port1.0.23   1015839      512            1
port1.0.24   1081377      512            1
lo           425997       512            1
po1          1179684      512            1
po2          1212453      512            1
sa3          1245222      512            1
```

Related Commands

show interface brief

show interface status

show interface switchport

show memory

Overview This command displays the memory used by each process that is currently running

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory [<stack-ID>] [sort {size|peak|stk}]
```

Parameter	Description	
`<stack-ID>`	Stack member number, from 1 to 8.	
`sort`	Changes the sorting order for the list of processes. If you do not specify this, then the list is sorted by percentage memory utilization.	
	`size`	Sort by the amount of memory the process is currently using.
	`peak`	Sort by the amount of memory the process is currently using.
	`stk`	Sort by the stack size of the process.

Mode User Exec and Privileged Exec

Usage If this command is entered on the stack master, it will display corresponding memory utilization information for all the stack members. A stack member heading will display the information for every stack member device.

Example To display the memory used by the current running processes, use the command:

```
awplus# show memory
```

Output Figure 6-9: Example output from the **show memory** command

```
awplus#show memory

Stack member 1:

RAM total: 514920 kB; free: 382716; buffers: 16368 kB

user processes
==============
pid name            mem%   size   peak   data   stk
962 pss                6  33112  36260  27696   244
1   init               0    348   1092    288    84
797 syslog-ng          0    816   2152    752    84
803 klogd              0    184   1244    124    84
843 inetd              0    256   1256    136    84
...
```

Table 4: Parameters in the output of the **show memory** command

Parameter	Description
Stack member	Stack member number.
`RAM total`	Total amount of RAM memory free.
`free`	Available memory size.
`buffers`	Memory allocated kernel buffers.
`pid`	Identifier number for the process.
`name`	Short name used to describe the process.
`mem%`	Percentage of memory utilization the process is currently using.
`size`	Amount of memory currently used by the process.
`peak`	Greatest amount of memory ever used by the process.
`data`	Amount of memory used for data.
`stk`	The stack size.

Related Commands

show memory allocations

show memory history

show memory pools

show memory shared

show memory allocations

Overview This command displays the memory allocations used by processes.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory allocations [<process>]
```

Parameter	Description
<process>	Displays the memory allocation used by the specified process.

Mode User Exec and Privileged Exec

Example To display the memory allocations used by all processes on your device, use the command:

```
awplus# show memory allocations
```

Output Figure 6-10: Example output from the **show memory allocations** command

```
awplus#show memory allocations
Memory allocations for imi
----------------------------

Current 15093760 (peak 15093760)

Statically allocated memory:
 - binary/exe                :    1675264
 - libraries                 :    8916992
 - bss/global data           :    2985984
 - stack                     :     139264

Dynamically allocated memory (heap):
 - total allocated           :    1351680
   - in use                  :    1282440
   - non-mmapped             :    1351680
 - maximum total allocated   :    1351680
 - total free space          :      69240
   - releasable              :      68968
   - space in freed fastbins :         16

Context
           filename:line   allocated      freed
 +            lib.c:749          484
.
.
.
```

Related Commands

show memory

show memory history

show memory pools

show memory shared

show tech-support

show memory history

Overview This command prints a graph showing the historical memory usage.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory history <stack-ID>
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.

Mode User Exec and Privileged Exec

Usage This command's output displays three graphs of the percentage memory utilization:

- per second for the last minute, then
- per minute for the last hour, then
- per 30 minutes for the last 30 hours.

If entered on the stack master, this command will display corresponding memory utilization information for all the stack members. A stack member heading will be displayed to distinguish the different lists for every stack member.

Examples To show a graph displaying the historical memory usage for either a single unstacked device, or a complete stack, use the command:

```
awplus# show memory history
```

To show a graph displaying the historical memory usage for specific stack member (stack member 2 in this example) within a stack, use the command:

```
awplus# show memory history 2
```

Output Figure 6-11: Example output from the **show memory history** command

```
STACK member 1:

Per minute memory utilization history

100
 90
 80
 70
 60
 50
 40************************************************************
 30
 20
 10
    |....|....|....|....|....|....|....|....|....|....|....|....
    Oldest                                                  Newest
        Memory utilization% per minute (last 60 minutes)
              * = average memory utilisation%.
...
```

Related Commands

show memory allocations

show memory pools

show memory shared

show tech-support

show memory pools

Overview This command shows the memory pools used by processes.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory pools [<process>]
```

Parameter	Description
<process>	Displays the memory pools used by the specified process.

Mode User Exec and Privileged Exec

Example To shows the memory pools used by processes, use the command:

```
awplus# show memory pools
```

Output Figure 6-12: Example output from the **show memory pools** command

```
awplus#show memory pools
Memory pools for imi
---------------------

Current 15290368 (peak 15290368)

Statically allocated memory:
 - binary/exe                :    1675264
 - libraries                 :    8916992
 - bss/global data           :    2985984
 - stack                     :     139264

Dynamically allocated memory (heap):
 - total allocated           :    1548288
   - in use                  :    1479816
   - non-mmapped             :    1548288
 - maximum total allocated   :    1548288
 - total free space          :      68472
   - releasable              :      68200
   - space in freed fastbins :         16
.
.
.
```

Related Commands

show memory allocations

show memory history

show tech-support

show memory shared

Overview This command displays shared memory allocation information. The output is useful for diagnostic purposes by Allied Telesis authorized service personnel.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show memory shared
```

Mode User Exec and Privileged Exec

Example To display information about the shared memory allocation used on the device, use the command:

```
awplus# show memory shared
```

Output Figure 6-13: Example output from the **show memory shared** command

```
awplus#show memory shared
Shared Memory Status
----------------------------
Segment allocated  = 39
Pages allocated    = 39
Pages resident     = 11

Shared Memory Limits
----------------------------
Maximum number of segments          = 4096
Maximum segment size (kbytes)       = 32768
Maximum total shared memory (pages) = 2097152
Minimum segment size (bytes)        = 1
```

Related Commands

show memory allocations

show memory history

show memory

show process

Overview This command lists a summary of the current running processes.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax show process [<*stack-ID*>] [sort {cpu|mem}]

Parameter	Description	
<*stack-ID*>	Stack member number, from 1 to 8.	
sort	Changes the sorting order for the list of processes.	
	cpu	Sorts the list by the percentage of CPU utilization.
	mem	Sorts the list by the percentage of memory utilization.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

Example To display a summary of the current running processes, use the command:

```
awplus# show process
```

To display a summary of the current running processes on stack member 2, use the command:

```
awplus# show process 2
```

Output Figure 6-14: Example output from the **show process** command

```
Stack
member 2:

CPU load for 1 minute: 0%; 5 minutes: 3%; 15 minutes: 0%
RAM total: 514920 kB; free: 382600 kB; buffers: 16368 kB

user processes
==============
pid name         thrds  cpu%  mem%   pri  state  sleep%
962 pss             12     0     6    25  sleep       5
1   init             1     0     0    25  sleep       0
797 syslog-ng        1     0     0    16  sleep      88


kernel threads
==============
pid name         cpu%  pri  state  sleep%
71  aio/0        0     20   sleep  0
3   events/0     0     10   sleep  98
...
```

Table 5: Parameters in the output from the **show process** command

Parameter	Description
Stack member	Stack member number.
CPU load	Average CPU load for the given period.
RAM total	Total memory size.
free	Available memory.
buffers	Memory allocated to kernel buffers.
pid	Identifier for the process.
name	Short name to describe the process.
thrds	Number of threads in the process.
cpu%	Percentage of CPU utilization that this process is consuming.
mem%	Percentage of memory utilization that this process is consuming.
pri	Process priority.
state	Process state; one of “run”, “sleep”, “stop”, “zombie”, or “dead”.
sleep%	Percentage of time the process is in the sleep state.

Related Commands

show cpu

show cpu history

show reboot history

Overview Use this command to display the device's reboot history.

Syntax `show reboot history [<stack-ID>]`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.

Mode User Exec and Privileged Exec

Example To show the reboot history of stack member 2, use the command:

```
awplus# show reboot history 2
```

Output Figure 6-15: Example output from the **show reboot history** command

```
awplus#show
reboot history 2

Stack
member 2:

<date>     <time>    <type>      <description>
-----------------------------------------------
2014-01-10 01:42:04  Expected    User Request
2014-01-10 01:35:31  Expected    User Request
2014-01-10 01:16:25  Unexpected Rebooting due to critical process (network/nsm)
failure!
2014-01-10 01:11:04  Unexpected Rebooting due to critical process (network/nsm)
failure!
2014-01-09
20:46:40  Unexpected Rebooting due to VCS duplicate member-ID
2014-01-09 19:56:16  Expected    User Request
2010-01-09
20:36:06  Unexpected Rebooting due to VCS duplicate master (Continuous
reboot prevention)
2014-01-09 19:51:20  Expected    User Request
```

Table 6: Parameters in the output from the **show reboot history** command

Parameter	Description
Unexpected	Reboot is counted by the continuous reboot prevention feature if the reboot event occurs in the time period specified for continuous reboot prevention.
Expected	Reboot is not counted by continuous reboot prevention feature.

Table 6: Parameters in the output from the **show reboot history** command

Parameter	Description
`Continuous reboot prevention`	A continuous reboot prevention event has occurred. The action taken is configured with the **continuous-reboot-prevention** command. The next time period during which reboot events are counted begins from this event.
`User request`	User initiated reboot via the CLI.

Related Commands

show continuous-reboot-prevention

show tech-support

show router-id

Overview Use this command to show the Router ID of the current system.

Syntax

```
show router-id
```

Mode User Exec and Privileged Exec

Example To display the Router ID of the current system, use the command:

```
awplus# show router-id
```

Output Figure 6-16: Example output from the **show router-id** command

```
awplus>show router-id
Router ID: 10.55.0.2 (automatic)
```

show system

Overview This command displays general system information about the device, including the hardware, installed, memory, and software versions loaded. It also displays location and contact details when these have been set.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show system
```

Mode User Exec and Privileged Exec

Example To display configuration information, use the command:

```
awplus# show system
```

Usage For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

Output Figure 6-17: Example output from **show system**

```
awplus#show system
System Status                                      Mon Nov 16 08:42:16 2015

Board       ID  Bay     Board Name                          Rev   Serial number
-------------------------------------------------------------------------------
Base       386          IX5-28GPX                           X5-0  A25DD5002
PSU        335  PSU1    PWR800                              C-0   421LC7023
-------------------------------------------------------------------------------
RAM:  Total: 495756 kB Free: 391896 kB
Flash: 63.0MB Used: 45.5MB Available: 17.5MB
-------------------------------------------------------------------------------
Environment Status : Normal
Uptime             : 0 days 01:20:56
Bootloader version : 2.0.25

Current software : IX5-5.4.5-2.1.rel
Software version : 5.4.5-2.1
Build date : Thu Nov 12 12:11:29 NZDT 2015

Current boot config: flash:/default.cfg (file exists)

System Name
 awplus
System Contact
System Location
```

Related Commands show system environment

show system environment

Overview This command displays the current environmental status of your device and any attached PSU, XEM, or other expansion option. The environmental status covers information about temperatures, fans, and voltage.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show system environment
```

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display the information for all the stack members. A stack member heading will be displayed to distinguish the different information for every stack member.

Example To display the system's environmental status, use the command:

```
awplus# show system environment
```

Output Figure 6-18: Example output from the **show system environment** command

```
Stack Environment Monitoring Status

Stack member 1:

Overall Status: Normal

Resource ID: 1  Name: x510-28GTX
ID  Sensor (Units)                      Reading  Low Limit High Limit Status
1   Fan: Fan 1 (Rpm)                       4344       3000          -     Ok
2   Voltage: 1.8V (Volts)                 1.804      1.617      1.978     Ok
3   Voltage: 1.0V (Volts)                 0.995      0.896      1.099     Ok
4   Voltage: 3.3V (Volts)                 3.291      2.960      3.613     Ok
5   Voltage: 5.0V (Volts)                 5.066      4.477      5.498     Ok
6   Voltage: 1.2V (Volts)                 1.187      1.072      1.318     Ok
7   Temp: CPU (Degrees C)                    50        -10         90     Ok
```

Related Commands show system

show system interrupts

Overview Use this command to display the number of interrupts for each IRQ (Interrupt Request) used to interrupt input lines on a PIC (Programmable Interrupt Controller) on your device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show system interrupts
```

Mode User Exec and Privileged Exec

Example To display information about the number of interrupts for each IRQ in your device, use the command:

```
awplus# show system interrupts
```

Output Figure 6-19: Example output from the **show system interrupts** command

```
awplus#show system interrupts
           CPU0
  5:   10428098 Enabled     0           MIPS  linux-kernel-bde
  6:          0 Enabled     0           MIPS  bcma-usb-ohci:usb1, bcma-usb-ehci:usb2
  7:  300725368 Enabled     0           MIPS  timer
 18:  598364339 Enabled     0         MIPS-CC  bcma_i2c
 22:       4909 Enabled     0         MIPS-CC  serial
 31:          1 Enabled     0       MIPS-GPIO  GPIO-Ethernet PHY
 35:          2 Enabled     0       MIPS-GPIO  GPIO-ECO Button
 40:          4 Enabled     0       MIPS-GPIO  PSU Interrupt
 42:          0 Enabled     0       MIPS-GPIO  PSU2 power good
 43:          0 Enabled     0       MIPS-GPIO  PSU1 power good
ERR:          0
```

Related Commands show system environment

show system mac

Overview This command displays the physical MAC address available on a standalone switch, or a stack. This command also shows the virtual MAC address for a stack if the stack virtual MAC address feature is enabled with the stack virtual-mac or the stack enable command.

Syntax
```
show system mac
```

Mode User Exec and Privileged Exec

Usage This command also displays the virtual MAC address, if the VCStack virtual MAC address feature is enabled with the stack virtual-mac command.

For more information, see the VCStack Feature Overview and Configuration Guide.

Example To display the physical MAC address enter the following command:

```
awplus# show system mac
```

Output Figure 6-20: Example output from the **show system mac** command

```
awplus#show system mac
eccd.6d9d.4eed
```

Output Figure 6-21: Example output showing how to use the **stack virtual-mac** command and the **show system mac** command

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#stack virtual-mac
% Please check that the new MAC 0000.cd37.0065 is unique within
the network.
% Save the config and restart the system for this change to take
effect.
Member1#copy run start
Building configuration...
[OK]
Member1#reload
reboot system? (y/n): y

        ... Rebooting at user request ...
Loading default configuration ....

awplus login: manager
Password:

awplus>show system mac
eccd.6d9d.4eed

Virtual MAC Address 0000.cd37.0065
```

Related Commands stack virtual-mac

show system pci device

Overview Use this command to display the PCI devices on your device.

Syntax

```
show system pci device
```

Mode User Exec and Privileged Exec

Example To display information about the PCI devices on your device, use the command:

```
awplus# show system pci device
```

Output Figure 6-22: Example output from the **show system pci device** command

```
awplus#show system pci device
00:0c.0 Class 0200: 11ab:00d1 (rev 01)
        Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 113
        Memory at 5ffff000 (32-bit, non-prefetchable) [size=4K]
        Memory at 58000000 (32-bit, non-prefetchable) [size=64M]

00:0d.0 Class 0200: 11ab:00d1 (rev 01)
        Flags: bus master, 66Mhz, medium devsel, latency 128, IRQ 116
        Memory at 57fff000 (32-bit, non-prefetchable) [size=4K]
        Memory at 50000000 (32-bit, non-prefetchable) [size=64M]
```

```
Member1#show system pci device
00:00.0 Class 0600: 14e4:5300 (rev 01)
        Subsystem: 14e4:5300
        Flags: bus master, fast devsel, latency 0, IRQ 5
        Memory at 18000000 (64-bit, non-prefetchable) [size=16K]
        Memory at <unassigned> (64-bit, non-prefetchable) [size=128M]
        Capabilities: [40] Power Management version 3
        Capabilities: [58] #09 [0078]
        Capabilities: [48] Message Signalled Interrupts: 64bit+ Queue=0/0 Enable
-
        Capabilities: [d0] #10 [0041]

00:01.0 Class 0200: 14e4:b321 (rev 12)
        Subsystem: 14e4:4d4c
        Flags: bus master, fast devsel, latency 0, IRQ 5
        Memory at 08000000 (64-bit, non-prefetchable) [size=256K]
        Capabilities: [48] Power Management version 3
        Capabilities: [50] Vital Product Data
        Capabilities: [58] Message Signalled Interrupts: 64bit+ Queue=0/3 Enable
-
        Capabilities: [a0] #11 [0000]
        Capabilities: [ac] #10 [0002]
```

Related Commands show system environment

show system pci tree

show system pci tree

Overview Use this command to display the PCI tree on your device.

Syntax

```
show system pci tree
```

Mode User Exec and Privileged Exec

Example To display information about the PCI tree on your device, use the command:

```
awplus# show system pci tree
```

Output Figure 6-23: Example output from the **show system pci tree** command

```
awplus>show system pci tree
-[00]-+-0c.0  11ab:00d1
      \-0d.0  11ab:00d1
```

Related Commands

show system environment

show system pci device

show system serialnumber

Overview This command shows the serial number information for the device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show system serialnumber
```

Mode User Exec and Privileged Exec

Example To display the serial number information for the device, use the command:

```
awplus# show system serialnumber
```

Output Figure 6-24: Example output from the **show system serial number** command

```
awplus#show system serialnumber
45AX5300X
```

show tech-support

Overview This command generates system and debugging information for the device and saves it to a file. You can optionally limit the command output to display only information for a given protocol or feature.

The command generates a large amount of output, which is saved to a file in compressed format. The output file name can be specified by outfile option. If the output file already exists, a new file name is generated with the current time stamp. If the output filename does not end with ".gz", then ".gz" is appended to the filename. Since output files may be too large for Flash on the device we recommend saving files to external memory or a TFTP server whenever possible to avoid device lockup. This method is not likely to be appropriate when running the working set option of AMF across a range of physically separated devices.

Syntax

```
show tech-support
{all|[atmf|dhcpsn|epsr|igmp|ip|ipv6|mld|pim|stack|stp|system|t
acacs+]|[outfile <filename>]}
```

Parameter	Description
`all`	Display full information
`atmf`	Display ATMF- specific information
`dhcpsn`	Display DHCP Snooping specific information
`epsr`	Display EPSR specific information
`igmp`	Display IGMP specific information
`ip`	Display IP specific information
`ipv6`	Display IPv6 specific information
`mld`	Display MLD specific information
`outfile`	Output file name
`pim`	Display PIM related information
`stack`	Display stacking device information
`stp`	Display STP specific information
`system`	Display general system information
`tacacs+`	Display TACACS+ information
`|`	Output modifier
`>`	Output redirection
`>>`	Output redirection (append)
<filename>	Specifies a name for the output file. If no name is specified, this file will be saved as: tech-support.txt.gz.

Default Captures **all** information for the device.

By default the output is saved to the file 'tech-support.txt.gz' in the current directory. If this file already exists in the current directory then a new file is generated with the time stamp appended to the file name, for example 'tech-support20080109.txt.gz', so the last saved file is retained.

Usage This command is useful for collecting a large amount of information about all protocols or specific protocols on your device so that it can then be analyzed for troubleshooting purposes. The output of this command can be provided to technical support staff when reporting a problem.

Mode Privileged Exec

Examples show tech-support

```
awplus# show tech-support
```

speed (asyn)

Overview This command changes the console speed from the device. Note that a change in console speed is applied for subsequent console sessions. Exit the current session to enable the console speed change using the clear line console command.

Syntax

```
speed <console-speed-in-bps>
```

Parameter	Description
<console-speed-in-bps>	Console speed Baud rate in bps (bits per second).
1200	1200 Baud
2400	2400 Baud
9600	9600 Baud
19200	19200 Baud
38400	38400 Baud
57600	57600 Baud
115200	115200 Baud

Default The default console speed baud rate is 9600 bps.

Mode Line Configuration

Usage This command is used to change the console (asyn) port speed. Set the console speed to match the transmission rate of the device connected to the console (asyn) port on your device.

Example To set the terminal console (asyn0) port speed from the device to 57600 bps, then exit the session, use the commands:

```
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# speed 57600
awplus(config-line)# exit
awplus(config)# exit
awplus# exit
```

Then log in again to enable the change:

```
awplus login:
Password:
awplus>
```

Related Commands

clear line console

line

show running-config

show startup-config

speed

system territory (deprecated)

Overview This command has been deprecated in Software Version 5.4.4-0.1 and later. It now has no effect.

It is no longer useful to specify a system territory, so there is no alternative command.

terminal monitor

Overview Use this command to display debugging output on a terminal.

To display the cursor after a line of debugging output, press the Enter key.

Use the command **terminal no monitor** to stop displaying debugging output on the terminal, or use the timeout option to stop displaying debugging output on the terminal after a set time.

Syntax

```
terminal monitor [<1-60>]
terminal no monitor
```

Parameter	Description
<1-60>	Set a timeout between 1 and 60 seconds for terminal output.

Default Disabled

Mode User Exec and Privileged Exec

Examples To display debugging output on a terminal, enter the command:

```
awplus# terminal monitor
```

To specify timeout of debugging output after 60 seconds, enter the command:

```
awplus# terminal monitor 60
```

To stop displaying debugging output on the terminal, use the command:

```
awplus# terminal no monitor
```

Related Commands All debug commands

undebug all

Overview This command applies the functionality of the no debug all command.

7 Pluggables and Cabling Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure and monitor Pluggables and Cabling, including:

- Cable Fault Locator for finding faults in copper cabling
- Optical Digital Diagnostic Monitoring (DDM) to help find fiber issues when links go down
- Active Fiber Monitoring for detecting changes in optical power received over fiber cables.

For more information, see the Pluggables and Cabling Feature Overview and Configuration_Guide.

Command List

clear test cable-diagnostics tdr

Overview This command clears the results of the last cable test that was run.

Syntax

```
clear test cable-diagnostics tdr
```

Mode Privileged Exec

Examples To clear the results of a previous cable-diagnostics test use the following commands:

```
awplus# clear test cable-diagnostics tdr
```

debug fiber-monitoring

Overview Use this command to enable debugging of active fiber monitoring on the specified ports.

Use the **no** variant of this command to disable debugging on all ports or the specified ports.

Syntax

```
debug fiber-monitoring interface <port-list>
no debug fiber-monitoring [interface <port-list>]
```

Parameter	Description
<port-list>	The list of fiber ports to enable or disable debugging for, as a single port, a comma separated list or a hyphenated range.

Default Debugging of active fiber monitoring is disabled by default.

Mode User Exec/Privileged Exec

Usage While debugging is enabled by this command for a port, all the optical power readings for the port are sent to the console.

Example To enable debugging messages for active fiber monitoring of port 1.0.2 to be sent to the console, use the commands:

```
awplus# debug fiber-monitoring interface port 1.0.2
awplus# terminal monitor
```

To disable debugging messages for active fiber monitoring on port 1.0.2, use the command:

```
awplus# no debug fiber-monitoring interface port 1.0.2
```

To disable all debugging messages for active fiber monitoring, use the command:

```
awplus# no debug fiber-monitoring
```

Output Figure 7-1: Example output from **debug fiber-monitoring**

```
awplus#debug fiber-monitoring interface port2.0.1
awplus#terminal monitor
% Warning: Console logging enabled
awplus#01:42:50 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1
Reading:1748 Baseline:1708 Threshold:1356
01:42:52 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1717
Baseline:1709 Threshold:1357
01:42:54 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1780
Baseline:1709 Threshold:1357
01:42:56 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1685
Baseline:1710 Threshold:1358
01:42:58 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1701
Baseline:1710 Threshold:1358
01:43:01 awplus Pluggable[522]: Fiber-monitor port2.0.1: Channel:1 Reading:1733
Baseline:1709 Threshold:1357
```

Related Commands show system fiber-monitoring

fiber-monitoring action

Overview Use this command to specify an action to be taken if the optical power received on the port changes from the baseline by the amount specified in the **fiber-monitoring sensitivity** command.

Use the **no** variant of this command to remove the specified action or all actions from the port.

Syntax

```
fiber-monitoring action {trap|shutdown}
no fiber-monitoring action [trap|shutdown]
```

Parameter	Description
`trap`	Send an SNMP notification.
`shutdown`	Shutdown the port.

Default By default a log message is generated, but no additional action is performed.

Mode Interface Configuration mode for a fiber port.

Usage If fiber monitoring is enabled and this command is not used to set an action, a change in received power on a fiber port only generates a log message.

Example To set the device to send an SNMP notification when ports 1.0.1 or 1.0.2 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# fiber-monitoring action trap
```

To set the device to send an SNMP notification and to shut down the port when ports 1.0.1 or 1.0.2 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# fiber-monitoring action trap shutdown
```

To set the device not to send an SNMP notification when ports 1.0.1 or 1.0.2 receive reduced power, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring action trap
```

To set the device not to perform any action when it receives reduced power on ports 1.0.1 or 1.0.2, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring action
```

Related Commands fiber-monitoring sensitivity

show system fiber-monitoring

fiber-monitoring baseline

Overview Use this command to configure how the baseline value for comparison is calculated for active fiber monitoring on the port.

Note that alarm generation will not commence until the link has been up for a full averaging period.

Use the **no** variant of this command to set the fiber-monitoring baseline to its default value.

Syntax

```
fiber-monitoring baseline (average <12-150>|fixed <1-65535>)
no fiber-monitoring baseline
```

Parameter	Description
`average`	Set the baseline optical power received to be based on the moving average of the specified number of most recent (non-zero) values. Default.
<12-150>	The number of most recent values to average for the baseline. Default: 12.
`fixed`	Set the baseline to a fixed level of received optical power. Not recommended—see Usage below.
<1-65535>	The fixed baseline value of received optical power in 0.0001mW.

Default The default is a moving average of the last 12 values. If the **fiber-monitoring interval** is set to its default (5s), the **fiber-monitoring baseline** default will be the average over the last minute.

Mode Interface Configuration for a fiber port

Usage ***CAUTION:*** *We do not recommend setting a fixed value because gradual change over time caused by temperature fluctuations, etc. could lead to unnecessary alarms.*

There are two ways to configure the baseline. The first is to choose a number of readings to average. This is the default and recommended method. The second is to set a fixed value in units of x0.0001mW.

If a fixed value is required, the easiest way is to enable fiber monitoring on the port and use the **show system fiber-monitoring** command to see what readings can be expected.

Example To set the baseline optical power to a moving average of the last 30 readings, use the command:

```
awplus(config-if)# fiber-monitoring baseline average 30
```

To set the baseline to its default, averaging the last 12 readings, use the command:

```
awplus(config-if)# no fiber-monitoring baseline
```

Related Commands

fiber-monitoring interval

fiber-monitoring sensitivity

fiber-monitoring enable

Overview Use this command to enable active fiber monitoring on a fiber port. If the port can support fiber monitoring but does not have the correct SFP or fiber type installed, the configuration will be saved, and monitoring will commence when a supported SFP is inserted. Disabling and re-enabling fiber monitoring on a port resets the baseline calculation.

Use the **no** variants of this command to disable active fiber monitoring on the interface, or to remove all the configuration and state for the ports, respectively.

Syntax

```
fiber-monitoring enable
no fiber-monitoring enable
no fiber-monitoring
```

Default Active fiber monitoring is disabled by default.

Mode Interface Configuration mode for a fiber port

Examples To enable active fiber monitoring on a ports 1.0.1 and 1.0.2, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# fiber-monitoring enable
```

To disable fiber monitoring on the ports, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring enable
```

To remove all fiber-monitoring configuration and state for the ports, use the commands:

```
awplus(config)# interface port1.0.1-1.0.2
awplus(config-if)# no fiber-monitoring
```

Related Commands

fiber-monitoring action

fiber-monitoring sensitivity

show system fiber-monitoring

fiber-monitoring interval

Overview Use this command to configure the fiber monitoring polling interval in seconds for the port. The optical power will be read every <interval> seconds and compared against the calculated threshold values to see if a log message or other action is required.

Use the **no** variant of this command to reset the polling interval to the default (5 seconds).

Syntax

```
fiber-monitoring interval <2-60>
no fiber-monitoring interval
```

Parameter	Description
<2-60>	Optical power polling interval in seconds.

Default The interval is set to 5 seconds by default.

Mode Interface configuration mode for a fiber port.

Example To set the fiber monitoring polling interval for port 1.0.2 to 30 seconds, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# fiber-monitoring interval 30
```

To reset the fiber monitoring polling interval back to the default (5s), use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# no fiber-monitoring interval
```

Related Commands fiber-monitoring baseline

show system fiber-monitoring

fiber-monitoring sensitivity

Overview Use this command to configure the sensitivity of the alarm thresholds on the port for active fiber monitoring.

Use the **no** variant of this command to reset the sensitivity to the default.

Syntax

```
fiber-monitoring sensitivity (low|medium|high|highest|fixed
<25-65535>)|relative <0.01-10.0>
```

```
no fiber-monitoring sensitivity
```

Parameter	Description
`low`	Low sensitivity (+/-2 dB)
`medium`	Medium sensitivity (1 dB) (default)
`high`	High sensitivity (the greater of 0.5 dB and 0.0025 mW)
`highest`	The highest sensitivity available: 0.0025mW
`fixed<25-65535>`	Fixed sensitivity at the specified level in 0.0001 mW.
`relative <0.01-10.0>`	Relative sensitivity at the specified level in dB.

Default The default is medium sensitivity.

Mode User Exec/Privileged Exec

Usage A log message is generated and configured actions are taken if the received optical power drops below the baseline value by the sensitivity configured with this command.

The sensitivity can be configured to one of four pre-defined levels in decibels or to a fixed absolute delta in units of 0.0001mW. The alarm thresholds can be seen in the **show system fiber-monitoring** output. The maximum absolute sensitivity configurable is 0.0025 mW. Note that 0.0025 mW equates to a reduction of approximately 1dB at the maximum attenuation of an AT-SPLX10/1.

Example To set the fiber monitoring sensitivity for port 1.0.2 to a relative sensitivity of 0.1 dB, use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# fiber-monitoring sensitivity relative 0.1
```

To reset the fiber monitoring sensitivity to the default (medium), use the commands:

```
awplus(config)# interface port1.0.2
awplus(config-if)# no fiber-monitoring sensitivity
```

Related Commands

fiber-monitoring action

fiber-monitoring baseline

show system fiber-monitoring

show system fiber-monitoring

Overview Use this command to display settings and current status for Active Fiber Monitoring.

Syntax

```
show system fiber-monitoring
```

Mode User Exec/Privileged Exec

Example To display configuration and status for active fiber monitoring on ports., use the command:

```
awplus# show system fiber-monitoring
```

Output Figure 7-2: Example output from **show system fiber-monitoring**

```
awplus#show sys fiber-monitoring
Fiber Monitoring Status
  Reading units 0.0001mW

Stack member 1:

Interface port1.0.1
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 35 values greater than 50
Status:
 Baseline value:   496
 Alarm threshold:  393
 Alarm:            no
 Last 12 Readings: 498 498 498 498 498 498 498 498 498 498 498 498
 Minimum reading: 486
 Maximum reading: 498

Interface port1.0.2
Status:           enabled
Supported:        Supported pluggable
Debugging:        disabled
Interval:         2 seconds
Sensitivity:      1.00dB
Baseline type:    average of last 30 values greater than 50
Status:
 Baseline value:   0
 Alarm threshold:  0
 Alarm:            no
 Last 12 Readings: 0 0 0 0 0 0 0 0 0 0 0 0
 Minimum reading: 0
 Maximum reading: 0
```

Table 7-1: Parameters in the output from **show system fiber-monitoring**

Parameter	Description
`Reading units`	The units for optical power readings in the rest of the display, e.g. 0.0001mW.
`Status`	Whether active fiber monitoring is enabled or disabled for this port.
`Supported`	Whether the pluggable inserted in this port supports active fiber monitoring.
`Debugging`	Whether debugging of active fiber monitoring is enabled or disabled for this port.
`Interval`	The configured interval between readings of optical power on this port.
`Sensitivity`	The configured sensitivity threshold for optical power changes on this port.
`Baseline type`	How the baseline optical power level is calculated: either the average of the specified number of previous readings or a specified fixed value in 0.0001mW.
`Status`	Current values for the following parameters.
`Baseline value`	The baseline value, calculated according to the configured baseline method, in 0.0001mW.
`Alarm threshold`	The current threshold for a change in optical power, calculated according to the configured sensitivity method, that will result in action.
`Alarm`	Whether the optical power at the most recent reading fallen below the threshold.
`Last 12 readings`	The last 12 optical power values measured, in 0.0001mW, with oldest value first.
`Minimum reading`	The lowest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.
`Maximum reading`	The highest optical power reading since the fiber pluggable was last inserted, or since active fiber monitoring was last enabled on the port.

Related Commands

debug fiber-monitoring

fiber-monitoring action

fiber-monitoring baseline

fiber-monitoring enable

fiber-monitoring interval

fiber-monitoring sensitivity

show system pluggable

Overview This command displays **brief** pluggable transceiver information showing the pluggable type, the pluggable serial number, and the pluggable port on the device. Different types of pluggable transceivers are supported in different models of device. See your Allied Telesis dealer for more information about the models of pluggables that your device supports.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax `show system pluggable [<port-list>]`

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.12`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.2.24`.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display information about the pluggable transceivers for all the stack members. A separate heading will be displayed to distinguish each stack member's information.

Example To display brief information about pluggable transceivers installed in `port1.0.1` through `port1.0.4`, use the command:

```
awplus# show system pluggable port1.0.1-1.0.4
```

Output Figure 7-3: Example output from the **show system pluggable port1.0.1-1.0.4** command

```
System Pluggable Information
Port   Manufacturer     Device           Serial Number    Datecode Type
-------------------------------------------------------------------------------
1.0.1  AGILENT          HFBR-5710L       0401312315461272 040131   1000BASE-SX
1.0.2  AGILENT          QBCU-5730R       AK0614GKF7       060408   1000BASE-T
1.0.3  AGILENT          HFBR-5710L       0305130112182696 030513   1000BASE-SX
1.0.4  AGILENT          HBCU-5710R       AK051300SM       050402   1000BASE-T
-------------------------------------------------------------------------------
```

Example To display information about the pluggable transceiver installed in `port1.0.1`, use the command:

```
awplus# show system pluggable port1.0.1
```

Output Figure 7-4: Example output from the **show system pluggable port1.0.1** command

```
System Pluggable Information
Port   Manufacturer     Device           Serial Number    Datecode Type
-------------------------------------------------------------------------------
1.0.1  AGILENT          HFBR-5710L       0401312315461272 040131   1000BASE-SX
-------------------------------------------------------------------------------
```

Related Commands

show system environment

show system pluggable detail

show system pluggable diagnostics

show system pluggable detail

Overview This command displays detailed pluggable transceiver information showing the pluggable type, the pluggable serial number, and the pluggable port on the device. Different types of pluggable transceivers are supported in different models of device. See your Allied Telesis dealer for more information about the models of pluggables that your device supports.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show system pluggable [<port-list>] detail
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.12`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.2.24`.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display detailed information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish the different pluggable transceiver information for every stack member.

In addition to the information about pluggable transceivers displayed using the show system pluggable command (port, manufacturer, serial number, manufacturing datecode, and type information), the **show system pluggable detail** command displays the following information:

- **SFP Laser Wavelength**: Specifies the laser wavelength of the installed pluggable transceiver
- **Single mode Fiber**: Specifies the link length supported by the pluggable transceiver using single mode fiber
- **OM1 (62.5µ m) Fiber**: Specifies the link length, in meters (m) or kilometers (km) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
- **OM2 (50µ m) Fiber**: Specifies the link length (in meters or kilometers) supported by the pluggable transceiver using 50 micron multi-mode fiber.

- **Diagnostic Calibration**: Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration.
  - **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration.
  - **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration.
  - **-** is displayed neither Internal Calibration or External Calibration is supported.
- **Power Monitoring**: Displays the received power measurement type, which can be either **OMA**(Optical Module Amplitude) or **Avg**(Average Power) measured in µW.

NOTE: *For parameters that are not supported or not specified, a hyphen is displayed instead.*

Example To display detailed information about the pluggable transceivers installed in a particular port on the device, use a command like:

```
awplus# show system pluggable port1.0.24 detail
```

To display detailed information about all the pluggable transceivers installed on the device, use the command:

```
awplus# show system pluggable detail
```

Output Figure 7-5: Example output from the **show system pluggable detail** command on a device

```
awplus#show system pluggable port1.0.24 detail
System Pluggable Information Detail

Port1.0.24
==========
Vendor Name:               AGILENT
Device Name:               HFCT-5710L
Device Revision:           A
Device Type:               1000BASE-LX
Serial Number:             0402142241184360
Manufacturing Datecode:    040214
SFP Laser Wavelength:      -
Link Length Supported
 Single Mode Fiber :      10Km
 OM1 (62.5um) Fiber:      550m
 OM2 (50um) Fiber  :      550m
Diagnostic Calibration:    Internal
Power Monitoring:          Avg
FEC BER support:           -
```

Example To display detailed information about the pluggable transceivers installed on a stack, use the command:

```
awplus# show system pluggable detail
```

Output Figure 7-6: Example output from the **show system pluggable detail** command on a stack

```
awplus#show system pluggable detail
System Pluggable Information Detail

Stack member 1:

Port1.0.24
==========
Vendor Name:              AGILENT
Device Name:              HFCT-5710L
Device Revision:          A
Device Type:              1000BASE-LX
Serial Number:            0402142241184360
Manufacturing Datecode:   040214
SFP Laser Wavelength:     -
Link Length Supported
 Single Mode Fiber :     10Km
 OM1 (62.5um) Fiber:     550m
 OM2 (50um) Fiber  :     550m
Diagnostic Calibration:   Internal
Power Monitoring:         Avg
FEC BER support:          -

Stack member 2:

Port2.0.24
==========
Vendor Name:              FINISAR CORP.
Device Name:              FTRJ-8519-7D-CSC
Device Revision:          A
Device Type:              1000BASE-SX
Serial Number:            P430KGY
Manufacturing Datecode:   030718
SFP Laser Wavelength:     850nm
Link Length Supported
  Single Mode Fiber :     -
  OM1 (62.5um) Fiber:     300m
  OM2 (50um) Fiber  :     550m
Diagnostic Calibration:   Internal
Power Monitoring:         OMA
FEC BER support:          Yes
```

Table 8: Parameters in the output from the **show system pluggables detail** command:

Parameter	Description
Stack member	The stack member number..
Port	Specifies the port the pluggable transceiver is installed in.
Vendor Name	Specifies the vendor's name for the installed pluggable transceiver.

Table 8: Parameters in the output from the **show system pluggables detail** command: (cont.)

Parameter	Description
Device Name	Specifies the device name for the installed pluggable transceiver.
Device Revision	Specifies the hardware revision code for the pluggable transceiver. This may be useful for troubleshooting because different devices may support different pluggable transceiver revisions.
Device Type	Specifies the device type for the installed pluggable transceiver..
Serial Number	Specifies the serial number for the installed pluggable transceiver.
Manufacturing Datecode	Specifies the manufacturing datecode for the installed pluggable transceiver. Checking the manufacturing datecode with the vendor may be useful when determining Laser Diode aging issues. For more information, see "How To Troubleshoot Fiber and Pluggable Issues" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.
SFP Laser Wavelength	Specifies the laser wavelength of the installed pluggable transceiver.
Single Mode Fiber	Specifies the link length supported by the pluggable transceiver using single mode fiber.
OM1 (62.5um) Fiber	Specifies the link length (in µm - micron) supported by the pluggable transceiver using 62.5 micron multi-mode fiber.
OM2 (50um) Fiber	Specifies the link length (in µm - micron) supported by the pluggable transceiver using 50 micron multi-mode fiber.
Diagnostic Calibration	Specifies whether the pluggable transceiver supports DDM or DOM Internal or External Calibration: **Internal** is displayed if the pluggable transceiver supports DDM or DOM Internal Calibration. **External** is displayed if the pluggable transceiver supports DDM or DOM External Calibration. **-** is displayed if neither Internal Calibration or External Calibration is supported.
Power Monitoring	Displays the received power measurement type, which can be either **OMA** (Optical Module Amplitude) or **Avg** (Average Power) measured in µW.

Related Commands

show system environment

show system pluggable

show system pluggable diagnostics

show system pluggable diagnostics

Overview This command displays diagnostic information about SFP and SFP+ pluggable transceivers that support Digital Diagnostic Monitoring (DDM).

Different types of pluggable transceivers are supported in different models of device. See your device's Datasheet for more information about the models of pluggables that your device supports.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show system pluggable [<port-list>] diagnostics
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.12`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.2.24`.

Mode User Exec and Privileged Exec

Usage For a stacked configuration, if this command is entered on the stack master, it will display information about the pluggable transceivers for all the stack members. A stack member heading will be displayed to distinguish different pluggable transceiver information for every stack member.

Usage Modern optical SFP and SFP+ transceivers support Digital Diagnostics Monitoring (DDM) functions.

Diagnostic monitoring features allow you to monitor real-time parameters of the pluggable transceiver, such as optical output power, optical input power, temperature, laser bias current, and transceiver supply voltage. Additionally, RX LOS (Loss of Signal) is shown when the received optical level is below a preset threshold. Monitor these parameters to check on the health of all transceivers, selected transceivers or a specific transceiver installed in a device.

Examples To display detailed information about all pluggable transceivers installed on a standalone device, use the command:

```
awplus# show system pluggable diagnostics
```

Output Figure 7-7: Example output from the **show system pluggable diagnostics** command on a device

```
awplus#show system pluggable diagnostics
System Pluggable Information Diagnostics

Port1.0.21          Status             Alarms                    Warnings
                  Reading   Alarm     Max      Min   Warning     Max      Min
Temp: (Degrees C)  29.387       -  100.00  -40.00         -  85.000  -10.00
Vcc: (Volts)        3.339       -    3.465   3.135        -    3.400   3.200
Tx Bias: (mA)      10.192       -   37.020   3.260        -   34.520   5.760
Tx Power: (mW)     17.872       -   35.643   8.953        -   28.313  11.271
Rx Power: (mW)      0.006     Low   15.849   0.025      Low   12.589   0.040
Rx LOS:           Rx Down

Port1.0.22          Status             Alarms                    Warnings
                  Reading   Alarm     Max      Min   Warning     Max      Min
Temp: (Degrees C)  29.387       -  100.00  -40.00         -  85.000  -10.00
Vcc: (Volts)        3.378       -    3.630   2.970        -    3.465   3.135
Tx Bias: (mA)       2.802       -    6.000   1.000        -    5.000   1.000
Tx Power: (mW)      2.900       -   11.000   0.600        -   10.000   0.850
Rx Power: (mW)      1.739       -   18.000   0.000        -   10.000   0.200
Rx LOS:             Rx Up
```

To display detailed information about the pluggable transceiver installed in `port1.0.22` on a standalone switch, use the command:

```
awplus# show system pluggable diagnostics port1.0.22
```

Table 9: Parameters in the output from the **show system pluggables diagnostics** command

Parameter	Description
Temp (Degrees C)	Shows the temperature inside the transceiver.
Vcc (Volts)	Shows voltage supplied to the transceiver.
Tx Bias (mA)	Shows current to the Laser Diode in the transceiver.
Tx Power (mW)	Shows the amount of light transmitted from the transceiver.
Rx Power (mW)	Shows the amount of light received in the transceiver.
Rx LOS	Rx Loss of Signal. This indicates whether: • light is being received (Rx Up) and therefore the link is up, or • light is not being received (Rx Down) and therefore the link is down

Related Commands

show system environment

show system pluggable

show system pluggable detail

show test cable-diagnostics tdr

Overview This command displays the results of the last cable-diagnostics test that was run using the TDR (Time Domain Reflectometer) on a fixed copper cable port.

The displayed status of the cable can be either:

- OK
- Open
- Short (within-pair)
- Short (across-pair)
- Error

Syntax

```
show test cable-diagnostics tdr
```

Mode Privileged Exec

Examples To show the results of a cable-diagnostics test use the following command:

```
awplus# show test cable-diagnostics tdr
```

Output Figure 7-8: Example output from the **show test cable-diagnostics tdr** command

```
Port     Pair  Length       Status
-----------------------------------------------
1.0.1    A     -            OK
         B     -            OK
         C     -            OK
         D     -            OK
```

test cable-diagnostics tdr interface

Overview This command applies the Cable Fault Locator's cable-diagnostics tests to twisted pair data cables for a selected port. The tests will detect either correct, short circuit, or open, circuit terminations. For more information on running the CFL, see the "Cable Fault Locator" Feature Overview and Configuration Guide.

The test can take several seconds to complete. See the related show command to display the test results.

A new test can only be started if no other test is in progress. CFL cannot run on a port that is currently supplying power via PoE.

The displayed status of the cable can be either, OK, Short (within-pair), or Open. The "Open" or "Short" status is accompanied with the distance from the source port to the incorrect termination.

Syntax

```
test cable-diagnostics tdr interface <interface>
```

Parameter	Description
cable-diagnostics	The cable diagnostic tests.
`tdr`	Time Domain Reflectometry.
`interface`	Selects the interface to test.
<interface>	Interface number of the port to be tested, i.e. 1.0.2.

Example To run a cable test on the cable inserted into port 1.0.1 use the following command:

```
awplus# test cable-diagnostics tdr interface port1.0.1
```

You will receive the following message:

```
Link will go down while test is in progress. Continue? (y/n): y
Select y to continue.
```

```
awplus# y
```

You will then receive the following message:

```
Test started. This will take several seconds to complete. Use
"show test cable-diagnostics tdr" to print results.
```

8 Logging Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure logging.

Command List

clear exception log

Overview This command resets the contents of the exception log, but does not remove the associated core files.

NOTE: *When this command is used within a stacked environment, it will remove the contents of the exception logs in all stack members.*

Syntax
```
clear exception log
```

Mode Privileged Exec

Example
```
awplus# clear exception log
```

clear log

Overview This command removes the contents of the buffered and permanent logs.

NOTE: *When this command is used within a stacked environment, it will remove the contents of the buffered and permanent logs in all stack members.*

Syntax

```
clear log
```

Mode Privileged Exec

Example To delete the contents of the buffered and permanent log use the command:

```
awplus# clear log
```

Validation Commands show log

Related Commands clear log buffered

clear log permanent

clear log buffered

Overview This command removes the contents of the buffered log.

NOTE: *When this command is used within a stacked environment, it will remove the contents of the buffered logs in all stack members.*

Syntax

```
clear log buffered
```

Mode Privileged Exec

Example To delete the contents of the buffered log use the following commands:

```
awplus# clear log buffered
```

Related Commands

default log buffered

log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log

show log config

clear log permanent

Overview This command removes the contents of the permanent log.

NOTE: *When this command is used within a stacked environment, it will remove the contents of the buffered logs in all stack members.*

Syntax

```
clear log permanent
```

Mode Privileged Exec

Example To delete the contents of the permanent log use the following commands:

```
awplus# clear log permanent
```

Related Commands

default log permanent

log permanent

log permanent (filter)

log permanent exclude

log permanent size

show log config

show log permanent

default log buffered

Overview This command restores the default settings for the buffered log stored in RAM. By default the size of the buffered log is 50 kB and it accepts messages with the severity level of “warnings” and above.

Syntax

```
default log buffered
```

Default The buffered log is enabled by default.

Mode Global Configuration

Example To restore the buffered log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log buffered
```

Related Commands

clear log buffered

log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log

show log config

default log console

Overview This command restores the default settings for log messages sent to the terminal when a log console command is issued. By default all messages are sent to the console when a **log console** command is issued.

Syntax

```
default log console
```

Mode Global Configuration

Example To restore the log console to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log console
```

Related Commands

log console

log console (filter)

log console exclude

show log config

default log email

Overview This command restores the default settings for log messages sent to an email address. By default no filters are defined for email addresses. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax

```
default log email <email-address>
```

Parameter	Description
<email-address>	The email address to send log messages to

Mode Global Configuration

Example To restore the default settings for log messages sent to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# default log email admin@alliedtelesis.com
```

Related Commands

log email

log email (filter)

log email exclude

log email time

show log config

default log host

Overview This command restores the default settings for log sent to a remote syslog server. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent. This command also restores the remote syslog server time offset value to local (no offset).

Syntax

```
default log host <ip-addr>
```

Parameter	Description
<ip-addr>	The IP address of a remote syslog server

Mode Global Configuration

Example To restore the default settings for messages sent to the remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# default log host 10.32.16.21
```

Related Commands

log host

log host (filter)

log host exclude

log host source

log host time

show log config

default log monitor

Overview This command restores the default settings for log messages sent to the terminal when a terminal monitor command is used.

Syntax

```
default log monitor
```

Default All messages are sent to the terminal when a terminal monitor command is used.

Mode Global Configuration

Example To restore the log monitor to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log monitor
```

Related Commands

log monitor (filter)

log monitor exclude

show log config

terminal monitor

default log permanent

Overview This command restores the default settings for the permanent log stored in NVS. By default, the size of the permanent log is 50 kB and it accepts messages with the severity level of `warnings` and above.

Syntax
```
default log permanent
```

Default The permanent log is enabled by default.

Mode Global Configuration

Example To restore the permanent log to its default settings use the following commands:

```
awplus# configure terminal
awplus(config)# default log permanent
```

Related Commands
clear log permanent
log permanent
log permanent (filter)
log permanent exclude
log permanent size
show log config
show log permanent

log buffered

Overview This command configures the device to store log messages in RAM. Messages stored in RAM are not retained on the device over a restart. Once the buffered log reaches its configured maximum allowable size old messages will be deleted to make way for new ones.

Syntax

```
log buffered
no log buffered
```

Default The buffered log is configured by default.

Mode Global Configuration

Examples To configured the device to store log messages in RAM use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered
```

To configure the device to not store log messages in a RAM buffer use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered
```

Related Commands

clear log buffered

default log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log

show log config

log buffered (filter)

Overview Use this command to create a filter to select messages to be sent to the buffered log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the buffered log.

Syntax

```
log buffered [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]

no log buffered [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages to the buffered log by severity level.	
<level>	The minimum severity of message to send to the buffered log. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages to the buffered log by program. Include messages from a specified program in the buffered log.	
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)

Parameter	Description	
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Filter messages to the buffered log by syslog facility.	
<*facility*>	Specify one of the following syslog facilities to include messages from in the buffered log:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
msgtext	Select messages containing a certain text string.	
<*text-string*>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default the buffered log has a filter to select messages whose severity level is "notices (5)" or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To add a filter to send all messages generated by EPSR that have a severity of **notices** or higher to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered level notices program epsr
```

To add a filter to send all messages containing the text *Bridging initialization*, to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered msgtext Bridging initialization
```

To remove a filter that sends all messages generated by EPSR that have a severity of **notices** or higher to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered level notices program epsr
```

To remove a filter that sends all messages containing the text *Bridging initialization*, to the buffered log use the following commands:

```
awplus# configure terminal
awplus(config)# no log buffered msgtext Bridging initialization
```

Related Commands

clear log buffered

default log buffered

log buffered

log buffered size

log buffered exclude

show log

show log config

log buffered exclude

Overview Use this command to exclude specified log messages from the buffered log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log buffered exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log buffered exclude [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. Either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output.	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)

Parameter	Description	
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
msgtext	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered exclude msgtext example of
irrelevant message
```

Related Commands clear log buffered

default log buffered

log buffered size

Overview This command configures the amount of memory that the buffered log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Syntax

```
log buffered size <50-250>
```

Parameter	Description
<50-250>	Size of the RAM log in kilobytes

Mode Global Configuration

Example To allow the buffered log to use up to 100 kB of RAM use the following commands:

```
awplus# configure terminal
awplus(config)# log buffered size 100
```

Related Commands

clear log buffered

default log buffered

log buffered

log buffered (filter)

log buffered exclude

show log

show log config

log console

Overview This command configures the device to send log messages to consoles. The console log is configured by default to send messages to the device's main console port.

Use the **no** variant of this command to configure the device not to send log messages to consoles.

Syntax

```
log console
no log console
```

Mode Global Configuration

Examples To configure the device to send log messages use the following commands:

```
awplus# configure terminal
awplus(config)# log console
```

To configure the device not to send log messages in all consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console
```

Related Commands

default log console

log console (filter)

log console exclude

show log config

log console (filter)

Overview This command creates a filter to select messages to be sent to all consoles when the **log console** command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax

```
log console [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]
```

```
no log console [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring

Parameter	Description	
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default the console log has a filter to select messages whose severity level is `critical` or higher. This filter may be removed using the **no** variant of this command. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples To create a filter to send all messages generated by MSTP that have a severity of `info` or higher to console instances where the log console command has been given, remove the default filter that includes everything use the following commands:

```
awplus# configure terminal
awplus(config)# log console level info program mstp
```

and then use the command:

```
awplus(config)# log console level info program mstp
```

To create a filter to send all messages containing the text "`Bridging initialization`" to console instances where the log console command has been given use the following commands:

```
awplus# configure terminal
awplus(config)# log console msgtext "Bridging initialization"
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to consoles use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level notices program epsr
```

To remove a default filter that includes sending `critical`, `alert` and `emergency` level messages to the console use the following commands:

```
awplus# configure terminal
awplus(config)# no log console level critical
```

Related Commands

default log console

log console

log console exclude

show log config

log console exclude

Overview Use this command to prevent specified log messages from being sent to the console, when console logging is turned on. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. Either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output.	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)

Parameter	Description	
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log console exclude msgtext example of
irrelevant message
```

Related Commands default log console

log email

Overview This command configures the device to send log messages to an email address. The email address is specified in this command.

Syntax

```
log email <email-address>
```

Parameter	Description
<email-address>	The email address to send log messages to

Default By default no filters are defined for email log targets. Filters must be defined before messages will be sent.

Mode Global Configuration

Example To have log messages emailed to the email address `admin@alliedtelesis.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com
```

Related Commands

default log email

log email (filter)

log email exclude

log email time

show log config

log email (filter)

Overview This command creates a filter to select messages to be sent to an email address. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a specified email address. All configuration relating to this log target will be removed.

Syntax

```
log email <email-address> [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

```
no log email <email-address> [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
<email-address>	The email address to send logging messages to	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)

Parameter	Description	
	imi	Integrated Management Interface (IMI)
	imish	Integrated Management Interface Shell (IMISH)
	epsr	Ethernet Protection Switched Rings (EPSR)
	rmon	Remote Monitoring
	loopprot	Loop Protection
	poe	Power-inline (Power over Ethernet)
	dhcpsn	DHCP snooping (DHCPSN)
facility	Filter messages by syslog facility.	
<*facility*>	Specify one of the following syslog facilities to include messages from:	
	kern	Kernel messages
	user	Random user-level messages
	mail	Mail system
	daemon	System daemons
	auth	Security/authorization messages
	syslog	Messages generated internally by syslogd
	lpr	Line printer subsystem
	news	Network news subsystem
	uucp	UUCP subsystem
	cron	Clock daemon
	authpriv	Security/authorization messages (private)
	ftp	FTP daemon
msgtext	Select messages containing a certain text string.	
<*text-string*>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Mode Global Configuration

Examples To create a filter to send all messages generated by EPSR that have a severity of `notices` or higher to the email address `admin@homebase.com` use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com level notices program epsr
```

To create a filter to send all messages containing the text "Bridging initialization", to the email address admin@homebase.com use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@homebase.com msgtext "Bridging initialization"
```

To create a filter to send messages with a severity level of informational and above to the email address admin@alliedtelesis.com use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@alliedtelesis.com level informational
```

To stop the device emailing log messages emailed to the email address admin@alliedtelesis.com use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@homebase.com
```

To remove a filter that sends all messages generated by EPSR that have a severity of notices or higher to the email address admin@homebase.com use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@homebase.com level notices program epsr
```

To remove a filter that sends messages with a severity level of informational and above to the email address admin@alliedtelesis.com use the following commands:

```
awplus# configure terminal
awplus(config)# no log email admin@alliedtelesis.com level informational
```

Related Commands

default log email

log email

log email exclude

log email time

show log config

log email exclude

Overview Use this command to prevent specified log messages from being emailed, when the device is configured to send log messages to an email address. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log email exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log email exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. Either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output.	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)

Parameter	Description	
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log email exclude msgtext example of irrelevant message
```

Related Commands

default log email

log email

log email (filter)

log email time

show log config

log email time

Overview This command configures the time used in messages sent to an email address. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax

```
log email <email-address> time {local|local-offset|utc-offset
{plus|minus}<0-24>}
```

Parameter	Description
<email-address>	The email address to send log messages to
`time`	Specify the time difference between the email recipient and the device you are configuring.
`local`	The device is in the same time zone as the email recipient
`local-offset`	The device is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from local time of the device to the email recipient in hours.
`utc-offset`	The device is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
`plus`	Negative offset (difference) from the device to the email recipient.
`minus`	Positive offset (difference) from the device to the email recipient.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage Use the **local** option if the email recipient is in the same time zone as this device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the email recipient in hours. Messages will display the time they were generated on this device but converted to the time zone of the email recipient.

Examples

To send messages to the email address `test@home.com` in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local 0
```

To send messages to the email address `admin@base.com` with the time information converted to the time zone of the email recipient, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email admin@base.com time local-offset plus
3
```

To send messages to the email address `user@remote.com` with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log email user@remote.com time utc-offset minus
3
```

Related Commands

default log email

log email

log email (filter)

log email exclude

show log config

log facility

Overview Use this command to specify an outgoing syslog facility. This determines where the syslog server will store the log messages.

Use the **no** variant of this command to remove the facility.

Syntax

```
log facility
{kern|user|mail|daemon|auth|syslog|lpr|news|uucp|cron|authpriv
|ftp|local0|local1|local2|local3|local4|local5|local6|local7}
```

```
no log facility
```

Parameter	Description
`kern`	Kernel messages
`user`	User-level messages
`mail`	Mail system
`daemon`	System daemons
`auth`	Security/authorization messages
`syslog`	Messages generated internally by the syslog daemon
`lpr`	Line printer subsystem
`news`	Network news subsystem
`uucp`	UNIX-to-UNIX Copy Program subsystem
`cron`	Clock daemon
`authpriv`	Security/authorization (private) messages
`ftp`	FTP daemon
`local0`	Local use 0
`local1`	Local use 1
`local2`	Local use 2
`local3`	Local use 3
`local4`	Local use 4
`local5`	Local use 5
`local6`	Local use 6
`local7`	Local use 7

Default None (the outgoing syslog facility depends on the log message)

Mode Global Configuration

Example To specify a facility of local0, use the following commands:

```
awplus# configure terminal
awplus(config)# log facility local0
```

Related Commands show log config

log host

Overview This command configures the device to send log messages to a remote syslog server via UDP port 514. The IP address of the remote server must be specified. By default no filters are defined for remote syslog servers. Filters must be defined before messages will be sent.

Syntax

```
log host <ip-addr>
no log host <ip-addr>
```

Parameter	Description
<ip-addr>	The IP address of a remote syslog server in dotted decimal format A.B.C.D

Mode Global Configuration

Examples To configure the device to send log messages to a remote syslog server with IP address `10.32.16.99` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.99
```

To stop the device from sending log messages to the remote syslog server with IP address `10.32.16.99` use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.99
```

Related Commands

default log host

log host (filter)

log host exclude

log host source

log host time

show log config

log host (filter)

Overview This command creates a filter to select messages to be sent to a remote syslog server. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a substring within the message or a combination of some or all of these.

The **no** variant of this command configures the device to no longer send log messages to a remote syslog server. The IP address of the syslog server must be specified. All configuration relating to this log target will be removed.

Syntax

```
log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log host <ip-addr> [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
<ip-addr>	The IP address of a remote syslog server.	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)

Parameter	Description	
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Mode Global Configuration

Examples To create a filter to send all messages generated by EPSR that have a severity of `notices` or higher to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level notices program epsr
```

To create a filter to send all messages containing the text "`Bridging initialization`", to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 msgtext "Bridging
initialization"
```

To create a filter to send messages with a severity level of `informational` and above to the syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 level informational
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to a remote syslog server with IP address `10.32.16.21`use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 level notices program
epsr
```

To remove a filter that sends all messages containing the text "`Bridging initialization`", to a remote syslog server with IP address `10.32.16.21` use the following commands:

```
awplus# configure terminal
awplus(config)# no log host 10.32.16.21 msgtext "Bridging
initialization"
```

To remove a filter that sends messages with a severity level of `informational` and above to the syslog server with IP address `10.32.16.21`use the following commands:

```
awplusawpluls# configure terminal
awplus(config)# no log host 10.32.16.21 level informational
```

Related Commands

default log host

log host

log host exclude

log host source

log host time

show log config

log host exclude

Overview Use this command to prevent specified log messages from being sent to the remote syslog server, when log host is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log host exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log host exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. Either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output.	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)

Parameter	Description	
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log host exclude msgtext example of irrelevant message
```

Related Commands default log host

log host source

Overview Use this command to specify a source interface or IP address for the device to send syslog messages from. You can specify any one of an interface name, an IPv4 address or an IPv6 address.

This is useful if the device can reach the syslog server via multiple interfaces or addresses and you want to control which interface/address the device uses.

Use the **no** variant of this command to stop specifying a source interface or address.

Syntax

```
log host source {<interface-name>|<ipv4-addr>|<ipv6-addr>}
no log host source
```

Parameter	Description
<interface-name>	Specify the source interface name. You can enter a VLAN, eth interface or loopback interface.
<ipv4-add>	Specify the source IPv4 address, in dotted decimal notation (A.B.C.D).
<ipv6-add>	Specify the source IPv6 address, in X:X::X:X notation.

Default None (no source is configured)

Mode Global Configuration

Example To send syslog messages from 192.168.1.1, use the commands:

```
awplus# configure terminal
awplus(config)# log host source 192.168.1.1
```

Related Commands

default log host

log host

log host (filter)

log host exclude

log host time

show log config

log host time

Overview This command configures the time used in messages sent to a remote syslog server. If the syslog server is in a different time zone to your device then the time offset can be configured using either the **utc-offset** parameter option keyword or the **local-offset** parameter option keyword, where **utc-offset** is the time difference from UTC (Universal Time, Coordinated) and **local-offset** is the difference from local time.

Syntax

```
log host <email-address> time {local|local-offset|utc-offset
{plus|minus} <0-24>}
```

Parameter	Description
<email-address>	The email address to send log messages to
`time`	Specify the time difference between the email recipient and the device you are configuring.
`local`	The device is in the same time zone as the email recipient
`local-offset`	The device is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from local time of the device to the email recipient in hours.
`utc-offset`	The device is in a different time zone to the email recipient. Use the **plus** or **minus** keywords and specify the difference (offset) from UTC time of the device to the email recipient in hours.
`plus`	Negative offset (difference) from the device to the syslog server.
`minus`	Positive offset (difference) from the device to the syslog server.
<0-24>	World Time zone offset in hours

Default The default is **local** time.

Mode Global Configuration

Usage Use the **local** option if the remote syslog server is in the same time zone as the device. Messages will display the time as on the local device when the message was generated.

Use the **offset** option if the email recipient is in a different time zone to this device. Specify the time offset of the remote syslog server in hours. Messages will display the time they were generated on this device but converted to the time zone of the remote syslog server.

Examples To send messages to the remote syslog server with the IP address `10.32.16.21` in the same time zone as the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.21 time local 0
```

To send messages to the remote syslog server with the IP address `10.32.16.12` with the time information converted to the time zone of the remote syslog server, which is 3 hours ahead of the device's local time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.12 time local-offset plus 3
```

To send messages to the remote syslog server with the IP address `10.32.16.02` with the time information converted to the time zone of the email recipient, which is 3 hours behind the device's UTC time zone, use the following commands:

```
awplus# configure terminal
awplus(config)# log host 10.32.16.02 time utc-offset minus 3
```

Related Commands

default log host

log host

log host (filter)

log host exclude

log host source

show log config

log monitor (filter)

Overview This command creates a filter to select messages to be sent to the terminal when the terminal monitor command is given. Selection can be based on the priority/severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

Syntax

```
log monitor [level <level>] [program <program-name>] [facility
<facility>] [msgtext <text-string>]

no log monitor [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)

Parameter	Description	
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default there is a filter to select all messages. This filter may be removed and replaced by filters that are more selective.

Mode Global Configuration

Examples To create a filter to send all messages generated by MSTP that have a severity of `info` or higher to terminal instances where the terminal monitor command has been given use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor level info program mstp
```

To remove a filter that sends all messages generated by EPSR that have a severity of `notices` or higher to the terminal use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level notices program epsr
```

To remove a default filter that includes sending everything to the terminal use the following commands:

```
awplus# configure terminal
awplus(config)# no log monitor level debugging
```

Related Commands

default log monitor

log monitor exclude

show log config

terminal monitor

log monitor exclude

Overview Use this command to prevent specified log messages from being displayed on a terminal, when terminal monitor is enabled. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log console exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. Either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output.	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)

Parameter	Description	
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log monitor exclude msgtext example of
irrelevant message
```

Related Commands default log monitor

log monitor (filter)

show log config

terminal monitor

log permanent

Overview This command configures the device to send permanent log messages to non-volatile storage (NVS) on the device. The content of the permanent log is retained over a reboot. Once the permanent log reaches its configured maximum allowable size old messages will be deleted to make way for new messages.

The **no** variant of this command configures the device not to send any messages to the permanent log. Log messages will not be retained over a restart.

Syntax

```
log permanent
no log permanent
```

Mode Global Configuration

Examples To enable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent
```

To disable permanent logging use the following commands:

```
awplus# configure terminal
awplus(config)# no log permanent
```

Related Commands

clear log permanent

default log permanent

log permanent (filter)

log permanent exclude

log permanent size

show log config

show log permanent

log permanent (filter)

Overview This command creates a filter to select messages to be sent to the permanent log. Selection can be based on the priority/ severity of the message, the program that generated the message, the logging facility used, a sub-string within the message or a combination of some or all of these.

The **no** variant of this command removes the corresponding filter, so that the specified messages are no longer sent to the permanent log.

Syntax

```
log permanent [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

```
no log permanent [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Filter messages sent to the permanent log by severity level.	
<level>	The minimum severity of message to send. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Filter messages by program. Include messages from a specified program.	
<program-name>	The name of a program to log messages from, either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output:	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)

Parameter	Description	
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Filter messages by syslog facility.	
<facility>	Specify one of the following syslog facilities to include messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Select messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default By default the buffered log has a filter to select messages whose severity level is `notices (5)` or higher. This filter may be removed using the **no** variant of this command.

Mode Global Configuration

Examples To create a filter to send all messages generated by EPSR that have a severity of `notices` or higher to the permanent log use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent level notices program epsr
```

To create a filter to send all messages containing the text "`Bridging initialization`", to the permanent log use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent msgtext Bridging initialization
```

Related Commands

clear log permanent

default log permanent

log permanent

log permanent exclude

log permanent size

show log config

show log permanent

log permanent exclude

Overview Use this command to prevent specified log messages from being sent to the permanent log. You can exclude messages on the basis of:

- the priority/severity of the message
- the program that generated the message
- the logging facility used
- a sub-string within the message, or
- a combination of some or all of these.

Use the **no** variant of this command to stop excluding the specified messages.

Syntax

```
log permanent exclude [level <level>] [program <program-name>]
[facility <facility>] [msgtext <text-string>]

no log permanent exclude [level <level>] [program
<program-name>] [facility <facility>] [msgtext <text-string>]
```

Parameter	Description	
`level`	Exclude messages of the specified severity level.	
<level>	The severity level to exclude. The level can be specified as one of the following numbers or level names, where 0 is the highest severity and 7 is the lowest severity:	
	`0|emergencies`	System is unusable
	`1|alerts`	Action must be taken immediately
	`2|critical`	Critical conditions
	`3|errors`	Error conditions
	`4|warnings`	Warning conditions
	`5|notices`	Normal, but significant, conditions
	`6|informational`	Informational messages
	`7|debugging`	Debug-level messages
`program`	Exclude messages from a specified program.	
<program-name>	The name of a program. Either one of the following predefined program names (not case-sensitive), or another program name (case-sensitive) that you find in the log output.	
	`rsvp`	Resource Reservation Protocol (RSVP)
	`dot1x`	IEEE 802.1X Port-Based Access Control
	`lacp`	Link Aggregation Control Protocol (LACP)
	`stp`	Spanning Tree Protocol (STP)
	`rstp`	Rapid Spanning Tree Protocol (RSTP)
	`mstp`	Multiple Spanning Tree Protocol (MSTP)

Parameter	Description	
	`imi`	Integrated Management Interface (IMI)
	`imish`	Integrated Management Interface Shell (IMISH)
	`epsr`	Ethernet Protection Switched Rings (EPSR)
	`rmon`	Remote Monitoring
	`loopprot`	Loop Protection
	`poe`	Power-inline (Power over Ethernet)
	`dhcpsn`	DHCP snooping (DHCPSN)
`facility`	Exclude messages from a syslog facility.	
<facility>	Specify one of the following syslog facilities to exclude messages from:	
	`kern`	Kernel messages
	`user`	Random user-level messages
	`mail`	Mail system
	`daemon`	System daemons
	`auth`	Security/authorization messages
	`syslog`	Messages generated internally by syslogd
	`lpr`	Line printer subsystem
	`news`	Network news subsystem
	`uucp`	UUCP subsystem
	`cron`	Clock daemon
	`authpriv`	Security/authorization messages (private)
	`ftp`	FTP daemon
`msgtext`	Exclude messages containing a certain text string.	
<text-string>	A text string to match (maximum 128 characters). This is case sensitive, and must be the last text on the command line.	

Default No log messages are excluded

Mode Global configuration

Example To remove messages that contain the string “example of irrelevant message”, use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent exclude msgtext example of
irrelevant message
```

Related Commands clear log permanent

default log permanent

log permanent size

Overview This command configures the amount of memory that the permanent log is permitted to use. Once this memory allocation has been filled old messages will be deleted to make room for new messages.

Syntax

```
log permanent size <50-250>
```

Parameter	Description
<50-250>	Size of the permanent log in kilobytes

Mode Global Configuration

Example To allow the permanent log to use up to 100 kB of NVS use the following commands:

```
awplus# configure terminal
awplus(config)# log permanent size 100
```

Related Commands

clear log permanent

default log permanent

log permanent

log permanent (filter)

log permanent exclude

show log config

show log permanent

log-rate-limit nsm

Overview This command limits the number of log messages generated by the device for a given interval.

Use the **no** variant of this command to revert to the default number of log messages generated by the device of up to 200 log messages per second.

Syntax

```
log-rate-limit nsm messages <message-limit> interval
<time-interval>
```

```
no log-rate-limit nsm
```

Parameter	Description
<message-limit>	<1-65535> The number of log messages generated by the device.
<time-interval>	<0-65535> The time period for log message generation in 1/100 seconds. If an interval of 0 is specified then no log message rate limiting is applied.

Default By default, the device will allow 200 log messages to be generated per second.

Mode Global Configuration

Usage Previously, if the device received a continuous stream of IGMP packets with errors, such as when a packet storm occurs because of a network loop, then the device generates a lot of log messages using more and more memory, which may ultimately cause the device to shutdown. This log rate limiting feature constrains the rate that log messages are generated by the device.

Note that if within the given time interval, the number of log messages exceeds the limit, then any excess log messages are discarded. At the end of the time interval, a single log message is generated indicating that log messages were discarded due to the log rate limit being exceeded.

Thus if the expectation is that there will be a lot of discarded log messages due to log rate limiting, then it is advisable to set the time interval to no less than 100, which means that there would only be one log message, indicating log excessive log messages have been discarded.

Examples To limit the device to generate up to 300 log messages per second, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# log-rate-limit nsm messages 300 interval 100
```

To return the device the default setting, to generate up to 200 log messages per second, use the following commands:

```
awplus# configure terminal
awplus(config)# no log-rate-limit nsm
```

show counter log

Overview This command displays log counter information.

Syntax

```
show counter log
```

Mode User Exec and Privileged Exec

Example To display the log counter information, use the command:

```
awplus# show counter log
```

Output Figure 8-1: Example output from the **show counter log** command

```
Log counters
Total Received        ......... 2328
Total Received P0     ......... 0
Total Received P1     ......... 0
Total Received P2     ......... 1
Total Received P3     ......... 9
Total Received P4     ......... 32
Total Received P5     ......... 312
Total Received P6     ......... 1602
Total Received P7     ......... 372
```

Table 1: Parameters in output of the **show counter log** command

Parameter	Description
Total Received	Total number of messages received by the log
Total Received P0	Total number of Priority 0 (Emergency) messages received
Total Received P1	Total number of Priority 1 (Alert) messages received
Total Received P2	Total number of Priority 2 (Critical) messages received
Total Received P3	Total number of Priority 3 (Error) messages received
Total Received P4	Total number of Priority 4 (Warning) messages received
Total Received P5	Total number of Priority 5 (Notice) messages received
Total Received P6	Total number of Priority 6 (Info) messages received
Total Received P7	Total number of Priority 7 (Debug) messages received

Related Commands show log config

show exception log

Overview This command displays the contents of the exception log. When used within a stacked environment, this command will display the contents of the exception log for all the stack members.

Syntax

```
show exception log
```

Mode User Exec and Privileged Exec

Example To display the exception log, use the command:

```
awplus# show exception log
```

Output Figure 8-2: Example output from the **show exception log** command on a device

```
awplus#show exception log

Stack member 1:

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2014 Jan 27 09:57:47 local7.debug awplus corehandler : Process imish (PID:3746)
signal 11, core dumped to /flash/imish-x610-5.4.3-3.7-1-1390816667-3746.tgz
2014 Jan 27 09:57:47 local7.debug awplus corehandler : Process imish (PID:2504)
signal 11, core dumped to /flash/imish-x610-5.4.3-3.7-1-1390816667-2504.tgz
2014 Jan 27 09:58:02 local7.debug awplus corehandler : Process ospfd (PID:1512)
signal 5, core dumped to /flash/ospfd-x610-5.4.3-3.7-1-1390816682-1512.tgz
------------------------------------------------------------------------
Stack member 2:

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2014 Jan 27 09:58:16 local7.debug awplus-2 corehandler : Process imi (PID:1427)
signal 5, core dumped to /flash/imi-x610-5.4.3-3.7-2-1390816696-1427.tgz
------------------------------------------------------------------------
```

show log

Overview This command displays the contents of the buffered log.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show log [tail [<10-250>]]
```

Parameter	Description
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default By default the entire contents of the buffered log is displayed.

Mode User Exec, Privileged Exec and Global Configuration

Usage If the optional **tail** parameter is specified only the latest 10 messages in the buffered log are displayed. A numerical value can be specified after the **tail** parameter to select how many of the latest messages should be displayed.

Examples To display the contents of the buffered log use the command:

```
awplus# show log
```

To display the 10 latest entries in the buffered log use the command:

```
awplus# show log tail 10
```

Output Figure 8-3: Example output from the **show log** command

```
awplus#show log

<date> <time> <facility>.<severity> <program[<pid>]>: <message>

------------------------------------------------------------------------
2011 Aug 29 07:55:22 kern.notice awplus kernel: Linux version 2.6.32.12-at1 (mak
er@awpmaker03-dl) (gcc version 4.3.3 (Gentoo 4.3.3-r3 p1.2, pie-10.1.5) ) #1 Wed
 Dec 8 11:53:40 NZDT 2010
2011 Aug 29 07:55:22 kern.warning awplus kernel: No pci config register base in
dev tree, using default
2011 Aug 29 07:55:23 kern.notice awplus kernel: Kernel command line: console=tty
S0,9600 releasefile=IX5-5.4.6-0.1.rel ramdisk=14688
bootversion=1.1.0-rc12 loglevel=1
 extraflash=00000000
2011 Aug 29 07:55:25 kern.notice awplus kernel: RAMDISK: squashfs filesystem fou
nd at block 0
2011 Aug 29 07:55:28 kern.warning awplus kernel: ipifwd: module license 'Proprie
tary' taints kernel.

.
.
.
```

Figure 8-4: Example output from the **show log tail** command

```
awplus#show log tail

<date> <time> <facility>.<severity> <program[<pid>]>: <message>

------------------------------------------------------------------------
2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 469 cmd logrotate /
etc/logrotate.conf

2006 Nov 10 13:30:01 cron.notice crond[116]: USER manager pid 471 cmd nbqueue --
wipe

2006 Nov 10 13:35:01 cron.notice crond[116]: USER manager pid 472 cmd nbqueue --
wipe

2006 Nov 10 13:40:01 cron.notice crond[116]: USER manager pid 477 cmd nbqueue --
wipe

2006 Nov 10 13:44:36 syslog.notice syslog-ng[67]: Log statistics;
processed=\'center(queued)=70\', processed=\'2006 Nov 10 13:45:01 cron.notice
crond[116]: USER manager pid 478 cmd logrotate /etc/logrotate.conf

2006 Nov 10 13:45:01 cron.notice crond[116]: USER manager pid 480 cmd nbqueue --
wipe

2006 Nov 10 13:49:32 syslog.notice syslog-ng[67]: SIGHUP received, reloading
configuration;

2006 Nov 10 13:50:01 cron.notice crond[116]: USER manager pid 482 cmd nbqueue --
wipe

2006 Nov 10 13:55:01 cron.notice crond[116]: USER manager pid 483 cmd nbqueue --
wipe

.
.
.
```

Related Commands

clear log buffered

default log buffered

log buffered

log buffered (filter)

log buffered size

log buffered exclude

show log config

show log config

Overview This command displays information about the logging system. This includes the configuration of the various log destinations, buffered, permanent, syslog servers (hosts) and email addresses. This also displays the latest status information for each of these destinations.

Syntax

```
show log config
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the logging configuration use the command:

```
awplus# show log config
```

Output Figure 8-5: Example output from the **show log config** command

```
Buffered log:
 Status ......... enabled
  Maximum size ... 100kb
  Filters:
 *1 Level ........ notices
    Program ...... any
    Facility ..... any
    Message text . any
  2 Level ........ informational
    Program ...... mstp
    Facility ..... daemon
    Message text . any
  Statistics ..... 1327 messages received, 821 accepted by filter (2015 Nov 11
10:36:16)
Permanent log:
  Status ......... enabled
  Maximum size ... 60kb
  Filters:
  1 Level ........ error
    Program ...... any
    Facility ..... any
    Message text . any
 *2 Level ........ warnings
    Program ...... dhcp
    Facility ..... any
    Message text . "pool exhausted"
  Statistics ..... 1327 messages received, 12 accepted by filter (2015 Nov 11
10:36:16)
```

```
Host 10.32.16.21:
  Time offset .... +2:00
  Offset type .... UTC
  Filters:
  1 Level ........ critical
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 1 accepted by filter (2015 Nov 11
10:36:16)
Email admin@alliedtelesis.com:
  Time offset .... +0:00
  Offset type .... Local
  Filters:
  1 Level ........ emergencies
    Program ...... any
    Facility ..... any
    Message text . any
  Statistics ..... 1327 messages received, 0 accepted by filter (2015 Nov 11
10:36:16)
...
```

In the above example the '*' next to filter 1 in the buffered log configuration indicates that this is the default filter. The permanent log has had its default filter removed, so none of the filters are marked with "*'.

NOTE: *Terminal log and console log cannot be set at the same time. If console logging is enabled then the terminal logging is turned off.*

Related Commands

show counter log

show log

show log permanent

show log permanent

Overview This command displays the contents of the permanent log.

When used within a stacked environment, this command will display the contents of the permanent log for all the stack members, unless you specify a particular stack member.

Syntax

```
show log permanent[<stack-ID>][tail [<10-250>]]
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.
`tail`	Display only the latest log entries.
<10-250>	Specify the number of log entries to display.

Default If the optional `tail` parameter is specified only the latest 10 messages in the permanent log are displayed. A numerical value can be specified after the `tail` parameter to select how many of the latest messages should be displayed.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the permanent log of stack member 2, use the command:

```
awplus# show log permanent 2
```

Output Figure 8-6: Example output from the **show log permanent** command

```
awplus#show log permanent 2

Stack member 2:

<date> <time> <facility>.<severity> <program[<pid>]>: <message>
------------------------------------------------------------------------
2014 Feb 25 09:10:48 daemon.crit awplus-2 HPI: HOTSWAP Pluggable 2.0.51 hotswapped
in: AT-StackXS/1.0
2014 Feb 25 09:10:48 daemon.crit awplus-2 HPI: HOTSWAP Pluggable 2.0.52 hotswapped
in: 2127931-2
2014 Feb 25 09:10:50 user.crit awplus-2 VCS[922]: Member 1 (eccd.6d7d.a50e) has
joined the stack
2014 Feb 25 09:10:52 user.crit awplus-2 VCS[922]: Member 1 (eccd.6d7d.a50e) has
become the Active Master
2014 Feb 25 09:10:52 local6.alert awplus-2 VCS[922]: stack member has booted from
non-default location, SW version auto synchronization cannot be supported.
2014 Feb 25 09:10:52 user.crit awplus-2 VCS[922]: Stack Virtual MAC is
0000.cd37.0002
2014 Feb 25 09:11:46 user.crit awplus-2 ATMF[862]: awplus-x510 has joined. 1
member in total.
```

Related Commands

clear log permanent

default log permanent

log permanent

log permanent (filter)

log permanent exclude

log permanent size

show log config

show running-config log

Overview This command displays the current running configuration of the Log utility.

Syntax

```
show running-config log
```

Mode Privileged Exec and Global Configuration

Example To display the current configuration of the log utility, use the command:

```
awplus# show running-config log
```

Related Commands show log

show log config

9 Scripting Commands

Introduction

Overview This chapter provides commands used for command scripts.

Command List

activate

Overview This command activates a script file.

Syntax

```
activate [background] <script>
```

Parameter	Description
`background`	Activate a script to run in the background. A process that is running in the background will operate as a separate task, and will not interrupt foreground processing. Generally, we recommend running short, interactive scripts in the foreground and longer scripts in the background. The default is to run the script in the foreground.
<script>	The file name of the script to activate. The script is a command script consisting of commands documented in this software reference. Note that you must use either a **. scp** or a **. sh** filename extension for a valid script text file, as described below in the usage section for this command.

Mode Privileged Exec

Usage When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an enable (Privileged Exec mode) command to the start of your script. If you need to run Global Configuration commands in your script you need to add a configure terminal command after the **enable** command at the start of your script.

The **activate** command executes the script in a new shell. A terminal length shell command, such as **terminal length 0** may also be required to disable a delay that would pause the display.

A script must be a text file with a filename extension of either **. sh** or **. scp** only for the AlliedWare Plus™ CLI to activate the script file. The **. sh** filename extension indicates the file is an ASH script, and the **. scp** filename extension indicates the file is an AlliedWare Plus™ script.

Examples To activate a command script to run as a background process, use the command:

```
awplus# activate background test.scp
```

Related Commands

configure terminal

echo

enable (Privileged Exec mode)

wait

echo

Overview This command echoes a string to the terminal, followed by a blank line.

Syntax

```
echo <line>
```

Parameter	Description
<line>	The string to echo

Mode User Exec and Privileged Exec

Usage This command may be useful in CLI scripts, to make the script print user-visible comments.

Example To echo the string `Hello World` to the console, use the command:

```
awplus# echo Hello World
```

Output

```
Hello World
```

Related Commands activate

wait

wait

Overview This command pauses execution of the active script for the specified period of time.

Syntax `wait <delay>`

Parameter	Description
<delay>	<1-65335> Specify the time delay in seconds

Default No wait delay is specified by default to pause script execution.

Mode Privileged Exec (when executed from a script not directly from the command line)

Usage Use this command to pause script execution in an . **scp** (AlliedWare Plus™ script) or an . **sh** (ASH script) file executed by the activate command. The script must contain an enable (Privileged Exec mode) command since the **wait** command is only executed in the Privileged Exec mode.When a script is activated, the privilege level is set to 1 enabling User Exec commands to run in the script. If you need to run Privileged Exec commands in your script you need to add an enable (Privileged Exec mode) command to the start of your script.

Example

Related Commands activate

echo

enable (Privileged Exec mode)

10 Interface Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure and display interfaces.

Command List

description (interface)

Overview Use this command to add a description to a specific port or interface.

Syntax

```
description <description>
```

Parameter	Description
<description>	Text describing the specific interface.

Mode Interface Configuration

Example The following example uses this command to describe the device that a switch port is connected to.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# description Boardroom PC
```

interface (to configure)

Overview Use this command to select one or more interfaces to configure.

Syntax

```
interface <interface-list>
interface lo
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface such as a VLAN (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`lo`	The local loopback interface.

Usage A local loopback interface is one that is always available for higher layer protocols to use and advertise to the network. Although a local loopback interface is assigned an IP address, it does not have the usual requirement of connecting to a lower layer physical entity. This lack of physical attachment creates the perception of a local loopback interface always being accessible via the network.

Local loopback interfaces can be utilized by a number of protocols for various purposes. They can be used to improve access to the device and also increase its reliability, security, scalability and protection. In addition, local loopback interfaces can add flexibility and simplify management, information gathering and filtering.

One example of this increased reliability is for OSPF to advertise a local loopback interface as an interface-route into the network irrespective of the physical links that may be “up” or “down” at the time. This provides a higher probability that the routing traffic will be received and subsequently forwarded.

Mode Global Configuration

Example The following example shows how to enter Interface mode to configure `vlan1`. Note how the prompt changes.

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)#
```

The following example shows how to enter Interface mode to configure the local loopback interface.

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)#
```

Related Commands

ip address (IP Addressing and Protocol)

show interface

show interface brief

mru

Overview Use this command to set the Maximum Receive Unit (MRU) size for switch ports, where MRU is the maximum frame size (excluding headers) that switch ports can receive. For more information, see the Switching Feature Overview and Configuration Guide.

Use the **no** variant of this command to remove a previously specified Maximum Receive Unit (MRU) size for switch ports, and restore the default MRU size (1500 bytes) for switch ports.

NOTE: *The figure of 1500 bytes specifies the payload only. For an IEEE 802.1q frame, provision is made (internally) for the following additional components:*

- Source and Destination addresses
- EtherType field
- Priority and VLAN tag fields
- FCS

These additional components increase the frame size internally to 1522 bytes.

Syntax

```
mru <mru-size>
no mru
```

Parameter	Description
<mru-size>	<68-16357> Specifies the Maximum Receive Unit (MRU) size in bytes, where 1500 bytes is the default Ethernet MRU size for an interface.

Default The default MRU size is 1500 bytes for switch ports.

Mode Interface Configuration for switch ports.

Usage Note that show interface output will only show MRU size for switch ports.

Examples To configure an MRU of 16357 bytes on `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# mru 16357
```

To configure an MRU of 1500 bytes on `port1.0.2` to `port1.0.4` use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# mru 1500
```

To restore the MRU size of 1500 bytes on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no mru
```

Related Commands show interface

mtu

Overview Use this command to set the Maximum Transmission Unit (MTU) size for VLANs, where MTU is the maximum packet size that VLANs can transmit. The MTU size setting is applied to both IPv4 and IPv6 packet transmission.

Use the **no** variant of this command to remove a previously specified Maximum Transmission Unit (MTU) size for VLANs, and restore the default MTU size (1500 bytes) for VLANs.

Syntax

```
mtu <68-1582>
no mtu
```

Default The default MTU size is 1500 bytes for VLAN interfaces.

Mode Interface Configuration for VLAN interfaces.

Usage If a device receives an IPv4 packet for Layer 3 switching to another VLAN with an MTU size smaller than the packet size, and if the packet has the '**don't fragment**' bit set, then the device will send an ICMP '**destination unreachable**' (3) packet type and a '**fragmentation needed and DF set**' (4) code back to the source. For IPv6 packets bigger than the MTU size of the transmitting VLAN interface, an ICMP '**packet too big**' (ICMP type 2 code 0) message is sent to the source.

Note that show interface output will only show MTU size for VLAN interfaces.

Examples To configure an MTU size of 1500 bytes on interface `vlan2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# mtu 1500
```

To configure an MTU size of 1500 bytes on interfaces `vlan2` to `vlan4`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# mtu 1500
```

To restore the MTU size to the default MTU size of 1500 bytes on `vlan2`, use the commands

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no mtu
```

To restore the MTU size to the default MTU size of 1500 bytes on `vlan2` and `vlan4`, use the commands

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no mtu
```

Related Commands show interface

show interface

Overview Use this command to display interface configuration and status.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface [<interface-list>]
show interface lo
```

Parameter	Description
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface such as a VLAN (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`lo`	The local loopback interface.

Mode User Exec and Privileged Exec

Usage Note that the output displayed with this command will show MTU (Maximum Transmission Unit) size for VLAN interfaces, and MRU (Maximum Received Unit) size for switch ports.

Example To display configuration and status information for all interfaces, use the command:

```
awplus# show interface
```

Figure 10-1: Example output from the **show interface** command

```
awplus#show interface
Interface port1.0.1
  Scope: both
  Link is UP, administrative state is UP
  Thrash-limiting
    Status Not Detected, Action link-down, Timeout 60(s)
  Hardware is Ethernet, address is 0000.cd24.daeb
  index 5001 metric 1 mru 1500
  <UP,BROADCAST,RUNNING,MULTICAST>
  current duplex full, current speed 1000
  configured duplex auto, configured speed auto, configured polarity auto
  current ecofriendly lpi
  configured ecofriendly lpi
  SNMP link-status traps: Sending (Suppressed after 20 traps in 60 sec.)
    input packets 2396, bytes 324820, dropped 0, multicast packets 2370
    output packets 73235, bytes 406566, multicast packets 7321 broadcast packets 7
  Time since last state change: 0 days 16:35:52

...

Interface lo
  Scope: both
  Link is UP, administrative state is UP
  Hardware is Loopback
  index 1 metric 1
  <UP,LOOPBACK,RUNNING>
  SNMP link-status traps: Disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 16:35:52

Interface vlan1
  Scope: both
  Link is DOWN, administrative state is UP
  Hardware is VLAN, address is 0000.cd24.daa8
  index 201 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,MULTICAST>
  VRF Binding: Not bound
  SNMP link-status traps: Disabled
  Bandwidth 1g
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 29, bytes 1334, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 05:36:40
```

To display configuration and status information for interface `lo`, use the command:

```
awplus# show interface lo
```

Figure 10-2: Example output from the **show interface lo** command

```
awplus#show interface lo
Interface lo
  Scope: both
  Link is UP, administrative state is UP
  Hardware is Loopback
  index 1 metric 1
  <UP,LOOPBACK,RUNNING>
  SNMP link-status traps: Disabled
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 0, bytes 0, multicast packets 0 broadcast packets 0
  Time since last state change: 69 days 01:28:47
```

To display configuration and status information for interfaces `vlan1` and `vlan2`, use the command:

```
awplus# show interface vlan1,vlan2
```

Figure 10-3: Example output from the **show interface vlan1,vlan2** command

```
awplus#show interface vlan1,vlan2
Interface vlan1
  Scope: both
  Link is UP, administrative state is UP
  Hardware is VLAN, address is 0015.77e9.5c50
  IPv4 address 192.168.1.1/24 broadcast 192.168.1.255
  index 201 metric 1 mtu 1500
  arp ageing timeout 300
<UP,BROADCAST,RUNNING,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
    input packets 295606, bytes 56993106, dropped 5, multicast packets 156
    output packets 299172, bytes 67379392, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 14:22:39

 Interface vlan2
  Scope: both
  Link is DOWN, administrative state is UP
  Hardware is VLAN, address is 0015.77e9.5c50
  IPv4 address 192.168.2.1/24 broadcast 192.168.2.255
  Description: ip_phone_vlan
  index 202 metric 1 mtu 1500
  arp ageing timeout 300
  <UP,BROADCAST,MULTICAST>
  SNMP link-status traps: Disabled
  Bandwidth 1g
    input packets 0, bytes 0, dropped 0, multicast packets 0
    output packets 90, bytes 4244, multicast packets 0 broadcast packets 0
  Time since last state change: 0 days 14:22:39
```

Related Commands

ecofriendly lpi

mru

mtu

show interface brief

show interface brief

Overview Use this command to display brief interface, configuration, and status information, including provisioning information.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show interface brief
```

Mode User Exec and Privileged Exec

Output Figure 10-4: Example output from the **show interface brief** command

```
awplus#show int brief
Interface              Status          Protocol
port1.0.1              admin up        down
port1.0.2              admin up        down
port1.0.3              admin up        down
port1.0.4              admin up        down
port1.0.5              admin up        down
port1.0.6              admin up        running
lo                     admin up        running
vlan1                  admin up        down
vlan2                  admin up        down
```

Table 1: Parameters in the output of the **show interface brief** command

Parameter	Description
`Interface`	The name or type of interface.
`Status`	The administrative state. This can be either **admin up** or **admin down**.
`Protocol`	The link state. This can be either **down**, **running**, or **provisioned**.

Related Commands

show interface

show interface memory

show interface status

Overview Use this command to display the status of the specified interface or interfaces. Note that when no interface or interfaces are specified then the status of all interfaces on the device are shown.

Syntax

```
show interface [<port-list>] status
```

Parameter	Description
<port-list>	The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.6`) a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Examples To display the status of ports 1.0.1 to 1.0.5, use the commands:

```
awplus# show interface port1.0.1-1.0.4 status
```

Table 2: Example output from the **show interface <port-list> status** command

```
awplus#show interface port1.0.1 -1.0.5 status
Port       Name               Status            Vlan Duplex   Speed Type
port1.0.1                     notconnect           1 auto      auto 1000BASE-T
port1.0.2                     notconnect           1 auto      auto 1000BASE-T
port1.0.3                     notconnect           1 auto      auto 1000BASE-T
port1.0.4                     notconnect           1 auto      auto 1000BASE-T
```

To display the status of all ports, use the commands:

```
awplus# show interface status
```

Table 3: Example output from the **show interface status** command

```
awplus#sho int status
Port      Name               Status             Vlan Duplex   Speed Type
port1.0.1 Trunk_Net          connected         trunk a-full  a-1000 1000BaseTX
port1.0.2 Access_Net1        connected             5 full       100 1000BaseTX
port1.0.3 Access_Net1        disabled              5 auto      auto 1000BaseTX
port1.0.4 Access_Net2        connected             6 a-half   a-100 1000BaseTX
port1.0.5 Private_Prom       connected            10 a-full   a-100 1000BaseTX
port1.0.6 Private_Net1       connected         10,11 a-full   a-100 1000BaseTX
port1.0.7 Private_Net2       connected         10,12 a-full   a-100 1000BaseTX
port1.0.8                    notconnect            1 auto      auto 1000BaseTX
.
.
port1.0.23
                  disabled              1 auto      auto not present
port1.0.24
                  notconnect            1 auto      auto unknown
sa1
                        notconnect        trunk auto      auto
```

Table 4: Parameters in the output from the **show interface status** command

Parameter	Description
Port	Name/Type of the interface.
Name	Description of the interface.
Status	The administrative and operational status of the interface; one of: • disabled: the interface is administratively down. • connect: the interface is operationally up. • notconnect: the interface is operationally down.
Vlan	VLAN type or VLAN IDs associated with the port: • When the VLAN mode is trunk, it displays **trunk** (it does not display the VLAN IDs). • When the VLAN mode is access, it displays the VLAN ID. • When the VLAN mode is private promiscuous, it displays the primary VLAN ID if it has one, and **promiscuous** if it does not have a VLAN ID. • When the VLAN mode is private host, it displays the primary and secondary VLAN IDs. • When the port is an Eth port, it displays **none**: there is no VLAN associated with it. • When the VLAN is dynamically assigned, it displays the current dynamically assigned VLAN ID (not the access VLAN ID), or **dynamic** if it has multiple VLANs dynamically assigned.

Table 4: Parameters in the output from the **show interface status** command

Parameter	Description
`Duplex`	The actual duplex mode of the interface, preceded by **a-** if it has autonegotiated this duplex mode. If the port is disabled or not connected, it displays the configured duplex setting.
`Speed`	The actual link speed of the interface, preceded by **a-** if it has autonegotiated this speed. If the port is disabled or not connected, it displays the configured speed setting.
`Type`	The type of interface, e.g. 1000BaseTX. For SFP bays, it displays **Unknown** if it does not recognize the type of SFP installed, or **Not present** if an SFP is not installed or is faulty.

Related Commands

show interface

show interface memory

shutdown

Overview This command shuts down the selected interface. This administratively disables the link and takes the link down at the physical (electrical) layer.

Use the **no** variant of this command to disable this function and therefore to bring the link back up again.

Syntax

```
shutdown
no shutdown
```

Mode Interface Configuration

Usage If you shutdown an aggregator, the device shows the admin status of the aggregator and its component ports as “admin down”. While the aggregator is down, the device accepts **shutdown** and **no shutdown** commands on component ports, but these have no effect on port status. Ports will not come up again while the aggregator is down.

Example To shut down port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# shutdown
```

To bring up port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no shutdown
```

To shut down vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# shutdown
```

To bring up vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no shutdown
```

11 Interface Testing Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used for testing interfaces.

Command List

clear test interface

Overview This command clears test results and counters after issuing a test interface command. Test results and counters must be cleared to issue subsequent test interface commands later on.

Syntax

```
clear test interface {<port-list>|all}
```

Parameter	Description
`<port-list>`	The ports to test. A port-list can be: • a switch port (e.g. `port1.0.6`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-port1.0.6` • a comma-separated list of the above, e.g. `port1.0.1,port1.0.5-1.0.6` The specified ports must exist.
`all`	All interfaces

Mode Privileged Exec

Examples To clear the counters for `port1.0.1` use the command:

```
awplus# clear test interface port1.0.1
```

To clear the counters for all interfaces use the command:

```
awplus# clear test interface all
```

Related Commands test interface

service test

Overview This command puts the device into the interface testing state, ready to begin testing. After entering this command, enter Interface Configuration mode for the desired interfaces and enter the command test interface.

Do not test interfaces on a device that is part of a live network—disconnect the device first.

Use the **no** variant of this command to stop the test service.

Syntax

```
service test
no service test
```

Mode Global Configuration

Example To put the device into a test state, use the command:

```
awplus(config)# service test
```

Related Commands test interface

test interface

Overview This command starts a test on a port or all ports or a selected range or list of ports.

Use the **no** variant of this command to disable this function. The test duration can be configured by specifying the time in minutes after specifying a port or ports to test.

For an example of all the commands required to test switch ports, see the Examples section in this command. To test the Eth port, set its speed to 100 by using the command **speed 100.**

NOTE: *Do not run test interface on live networks because this will degrade network performance.*

Syntax

```
test interface {<port-list>|all} [time{<1-60>|cont}]
no test interface {<port-list>|all}
```

Parameter	Description
<port-list>	The ports to test. A port-list can be: • a switch port (e.g. `port1.0.6`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-port1.0.6` • a comma-separated list of the above, e.g. `port1.0.1,port1.0.5-1.0.6` The specified ports must exist.
`all`	All ports
`time`	Keyword entered prior to the value for the time duration of the interface test.
<1-60>	Specifies duration of time to test the interface or interfaces in minutes (from a minimum of 1 minute to a maximum of 60 minutes). The default is 4 minutes.
`cont`	Specifies continuous interface testing until canceled with command negation.

Mode Privileged Exec

Example To test the switch ports in VLAN 1, install loopbacks in the ports, and enter the following commands:

```
awplus(config)# service test
awplus(config)# no spanning-tree rstp enable bridge-forward
awplus(config)# interface vlan1
awplus(config-if)# shutdown
awplus(config-if)# end
awplus# test interface all
```

To see the output, use the commands:

```
awplus# show test
awplus# show test count
```

To start the test on all interfaces for 1 minute use the command:

```
awplus# test interface all time 1
```

Related Commands clear test interface

Part 2: Layer Two Switching

12 Switching Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure switching.

For more information, see the Switching Feature Overview and Configuration Guide.

Command List

backpressure

Overview This command provides a method of applying flow control to ports running in half duplex mode. The setting will only apply when the link is in the half-duplex state.

You can disable backpressure on an interface using the **off** parameter or the **no** variant of this command.

Syntax

```
backpressure {on|off}
no backpressure
```

Parameters	Description
`on`	Enables half-duplex flow control.
`off`	Disables half-duplex flow control.

Default Backpressure is turned off by default. You can determine whether an interface has backpressure enabled by viewing the running-config output; **backpressure on** is shown for interfaces if this feature is enabled.

Mode Interface Configuration

Usage The backpressure feature enables half duplex Ethernet ports to control traffic flow during congestion by preventing further packets arriving. Back pressure utilizes a pre-802.3x mechanism in order to apply Ethernet flow control to switch ports that are configured in the half duplex mode.

The flow control applied by the flowcontrol (switch port) command operates only on full-duplex links, whereas back pressure operates only on half-duplex links.

If a port has insufficient capacity to receive further frames, the device will simulate a collision by transmitting a CSMACD jamming signal from this port until the buffer empties. The jamming signal causes the sending device to stop transmitting and wait a random period of time, before retransmitting its data, thus providing time for the buffer to clear. Although this command is only valid for switch ports operating in half-duplex mode the remote device (the one sending the data) can be operating in the full duplex mode.

To see the currently-negotiated duplex mode for ports whose links are up, use the command show interface. To see the configured duplex mode (when different from the default), use the command show running-config.

Examples To enable back pressure flow control on interfaces `port1.0.1-port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# backpressure on
```

To disable back pressure flow control on interface `port1.0.2` enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# backpressure off
```

Validation Commands

show running-config

show interface

Related Commands

duplex

clear loop-protection counters

Overview Use this command to clear the counters for the Loop Protection counters.

Syntax

```
clear loop-protection [interface <port-list>] counters
```

Parameters	Description
`interface`	The interface whose counters are to be cleared.
<port-list>	A port, a port range, or an aggregated link.

Mode Privileged Exec

Examples To clear the counter information for all interfaces:

```
awplus# clear loop-protection counters
```

To clear the counter information for a single port:

```
awplus# clear loop-protection interface port1.0.1 counters
```

clear mac address-table dynamic

Overview Use this command to clear the filtering database of all entries learned for a selected MAC address, an MSTP instance, a switch port interface or a VLAN interface.

Syntax
```
clear mac address-table dynamic [address
<mac-address>|interface <port> [instance <inst>]|vlan <vid>]
```

Parameter	Description
`address`	Specify a MAC (Media Access Control) address to be cleared from the filtering database.
`<mac-address>`	Enter a MAC address to be cleared from the database in the format HHHH.HHHH.HHHH.
`interface`	Specify a switch port to be cleared from the filtering database.
`instance`	Specify an MSTP (Multiple Spanning Tree) instance to be cleared from the filtering database.
`<inst>`	Enter an MSTP instance in the range 1 to 63 to be cleared from the filtering database.
`vlan`	Specify a VLAN to be cleared from the filtering database.
`<vid>`	Enter a VID (VLAN ID) in the range 1 to 4094 to be cleared from the filtering database.

Mode Privileged Exec

Usage Use this command with options to clear the filtering database of all entries learned for a given MAC address, interface or VLAN. Use this command without options to clear any learned entries.

Use the optional `instance` parameter to clear the filtering database entries associated with a specified MSTP instance Note that you must first specify a switch port interface before you can specify an MSTP instance.

Compare this usage and operation with the clear mac address-table static command. Note that an MSTP instance cannot be specified with the command **clear mac address-table static**.

Examples This example shows how to clear all dynamically learned filtering database entries for all interfaces, addresses, VLANs.

```
awplus# clear mac address-table dynamic
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for the MAC address 0000.5E00.5302.

```
awplus# clear mac address-table dynamic address 0000.5E00.5302
```

This example shows how to clear all dynamically learned filtering database entries when learned through device operation for a given MSTP instance `1` on switch port interface `port1.0.2`.

```
awplus# clear mac address-table dynamic interface port1.0.2
instance 1
```

Related Commands

clear mac address-table static

show mac address-table

clear mac address-table static

Overview Use this command to clear the filtering database of all statically configured entries for a selected MAC address, interface, or VLAN.

Syntax

```
clear mac address-table static [address <mac-address>|interface
<port>|vlan <vid>]
```

Parameter	Description
`address`	The MAC address whose entries are to be cleared from the filtering database.
`<mac-address>`	Specifies the MAC (Media Access Control) address to be cleared from. Enter this address in the format HHHH.HHHH.HHHH.
`interface`	Specify the interface from which statically configured entries are to be cleared.
`<port>`	Specify the switch port from which address entries will be cleared. This can be a single switch port, (e.g. port1.0.4), a static channel group (e.g. sa2), or a dynamic (LACP) channel group (e.g. po2).
`vlan`	A VLAN whose statically configured entries are to be cleared.
`<vid>`	Specifies the VLAN ID whose statically configured entries are to be cleared.

Mode Privileged Exec

Usage Use this command with options to clear the filtering database of all entries made from the CLI for a given MAC address, interface or VLAN. Use this command without options to clear any entries made from the CLI.

Compare this usage with clear mac address-table dynamic command.

Examples This example shows how to clear all filtering database entries configured through the CLI.

```
awplus# clear mac address-table static
```

This example shows how to clear all filtering database entries for a specific interface configured through the CLI.

```
awplus# clear mac address-table static interface port1.0.3
```

This example shows how to clear filtering database entries configured through the CLI for the mac address 0000.5E00.5302.

```
awplus# clear mac address-table static address 0000.5E00.5302
```

Related Commands

clear mac address-table dynamic

mac address-table static

show mac address-table

clear port counter

Overview Use this command to clear the packet counters of the port.

Syntax

```
clear port counter [<port>]
```

Parameter	Description
<port>	The port number or range

Mode Privileged Exec

Example To clear the packet counter for `port1.0.1`, use the command:

```
awplus#  clear port counter port1.0.1
```

Related Commands show platform port

clear port-security intrusion

Overview Use this command to clear the history of the port-security intrusion list on all ports, or an individual port. If a port is not specified, the intrusion lists of all ports are cleared. This command does not clear any MAC addresses the device has already learned on the ports. If you want to clear MAC addresses on a switch port from the filtering database, you can use the clear mac address-table dynamic command or the clear mac address-table static command.

Syntax

```
clear port-security intrusion  [interface <port>]
```

Parameter	Description
<port>	Specify the switch port from which the history of violated address entries will be cleared. The port can be a single switch port, (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Examples To see the port-security status on port1.0.1, use the following command:

```
awplus# show port-security interface port1.0.1
```

Table 1: Example output from the **show port-security interface** command

```
awplus#show port-security interface port1.0.1
Port Security configuration
------------------------------------------------------------
Security Enabled : YES
Port Status : ENABLED
Violation Mode : TRAP
Aging : OFF
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Lock Status : LOCKED
Security Violation Count : 1
Last Violation Source Address : 801f.0200.19da
```

To see the intrusion list on port1.0.1, use the following command:

```
awplus# show port-security intrusion interface port1.0.1
```

Table 2: Example output from the **show port-security intrusion** command

```
awplus#show port-security intrusion interface port1.0.1
Port Security Intrusion List
------------------------------------------------------------
Interface: port1.0.1     - 1 intrusion(s) detected
801f.0200.19da
```

To clear the history of port-security intrusion list on port1.0.1, use the following command:

```
awplus# clear port-security intrusion interface port1.0.1
```

To see the port-security status on port1.0.1, use the following command:

```
awplus# show port-security interface port1.0.1
```

Table 3: Example output from the **show port-security interface** command

```
awplus#show port-security interface port1.0.1
Port Security configuration
------------------------------------------------------------
Security Enabled : YES
Port Status : ENABLED
Violation Mode : TRAP
Aging : OFF
Maximum MAC Addresses : 1
Total MAC Addresses : 1
Lock Status : LOCKED
Security Violation Count : 0
Last Violation Source Address : None
```

NOTE: *Note that the port status is still locked while the history of port violation is cleared from the database.*

To see the intrusion list on port1.0.1, use the following command:

```
awplus# show port-security intrusion interface port1.0.1
```

Table 4: Example output from the **show port-security intrusion** command

```
awplus#show port-security intrusion interface port1.0.1
Port Security Intrusion List
------------------------------------------------------------
Interface: port1.0.1     - no intrusions detected
```

Related Commands

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security maximum

switchport port-security violation

debug loopprot

Overview This command enables Loop Protection debugging.

The **no** variant of this command disables Loop Protection debugging.

Syntax

```
debug loopprot {info|msg|pkt|state|nsm|all}
no debug loopprot {info|msg|pkt|state|nsm|all}
```

Parameter	Description
`info`	General Loop Protection information.
`msg`	Received and transmitted Loop Detection Frames (LDFs).
`pkt`	Echo raw ASCII display of received and transmitted LDF packets to the console.
`state`	Loop Protection states transitions.
`nsm`	Network Service Module information.
`all`	All debugging information.

Mode Privileged Exec and Global Configuration

Example To enable debug for all state transitions, use the command:

```
awplus#  debug loopprot state
```

Related Commands show debugging loopprot

undebug loopprot

debug platform packet

Overview This command enables platform to CPU level packet debug functionality on the device.

Use the **no** variant of this command to disable platform to CPU level packet debug. If the result means both send and receive packet debug are disabled, then any active timeout will be canceled.

Syntax

```
debug platform packet [recv] [send] [sflow] [timeout <timeout>]
[vlan <vlan-id>|all]
```

```
no debug platform packet [recv] [send]
```

Parameter	Description
`recv`	Debug packets received.
`send`	Debug packets sent.
`sflow`	Debug sFlow packets.
`timeout`	Stop debug after a specified time.
<timeout>	<0-3600>The timeout period, specified in seconds.
`vlan`	Limit debug to a single VLAN ID specified.
<vlan-id>	<1-4094> The VLAN ID to limit the debug output on.
`all`	Debug all VLANs (default setting).

Default A 5 minute timeout is configured by default if no other timeout duration is specified.

Mode Privileged Exec and Global Configuration

Usage This command can be used to trace packets sent and received by the CPU. If a timeout is not specified, then a default 5 minute timeout will be applied.

If a timeout of 0 is specified, packet debug will be generated until the **no** variant of this command is used or another timeout value is specified. The timeout value applies to both send and receive debug and is updated whenever the **debug platform packet** command is used.

Examples To enable both receive and send packet debug for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet
```

To enable receive packet debug for 10 seconds, enter:

```
awplus# debug platform packet recv timeout 10
```

To enable packet debug for sFlow packets only for the default timeout of 5 minutes, enter:

```
awplus# debug platform packet sflow
```

To enable send packet debug with no timeout, enter:

```
awplus# debug platform packet send timeout 0
```

To enable VLAN packet debug for VLAN 2 with a timeout duration of 3 minutes, enter:

```
awplus# debug platform packet vlan 2 timeout 150
```

To disable receive packet debug, enter:

```
awplus# no debug platform packet recv
```

Related Commands

show debugging platform packet

undebug platform packet

duplex

Overview This command changes the duplex mode for the specified port.

To see the currently-negotiated duplex mode for ports whose links are up, use the command show interface. To see the configured duplex mode (when different from the default), use the command show running-config.

Syntax

```
duplex {auto|full|half}
```

Parameter	Description
`auto`	Auto-negotiate duplex mode.
`full`	Operate in full duplex mode only.
`half`	Operate in half duplex mode only.

Default By default, ports auto-negotiate duplex mode (except for 100Base-FX ports which do not support auto-negotiation, so default to full duplex mode).

Mode Interface Configuration

Usage Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the duplex mode of all the switch ports in the channel group by applying this command to the channel group.

Examples To specify full duplex for `port1.0.4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex full
```

To specify half duplex for `port1.0.4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex half
```

To auto-negotiate duplex mode for `port1.0.4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# duplex auto
```

Related Commands

backpressure

polarity

speed

show interface

flowcontrol (switch port)

Overview Use this command to enable flow control, and configure the flow control mode for the switch port.

Use the **no** variant of this command to disable flow control for the specified switch port.

Syntax

```
flowcontrol {send|receive} {off|on}
no flowcontrol
```

Parameter	Description
`receive`	When the port receives pause frames, it temporarily stops (pauses) sending traffic.
`on`	Enable the specified flow control.
`off`	Disable the specified flow control.
`send`	When the port is congested (receiving too much traffic), it sends pause frames to request the other end to temporarily stop (pause) sending traffic.

Default By default, flow control is disabled.

Mode Interface Configuration

Usage The flow control mechanism specified by 802.3x is only for full duplex links. It operates by sending PAUSE frames to the link partner to temporarily suspend transmission on the link

Flow control enables connected Ethernet ports to control traffic rates during congestion by allowing congested nodes to pause link operation at the other end. If one port experiences congestion, and cannot receive any more traffic, it notifies the other port to stop sending until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. On receiving a pause frame, the remote device stops sending data packets, which prevents loss of data packets during the congestion period.

Flow control is not recommended when running QoS or ACLs, because the complex queuing, scheduling, and filtering configured by QoS or ACLs may be slowed by applying flow control.

For half-duplex links, an older form of flow control known as backpressure is supported. See the related backpressure command.

For flow control on async serial (console) ports, see the flowcontrol hardware (asyn/console) command.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive on
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send on
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol receive off
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# flowcontrol send off
```

Validation Commands show running-config

Related Commands backpressure

linkflap action

Overview Use this command to detect flapping on all ports. If more than 15 flaps occur in less than 15 seconds the flapping port will shut down.

Use the **no** variant of this command to disable flapping detection at this rate.

Syntax

```
linkflap action [shutdown]
no linkflap action
```

Parameter	Description
`linkflap`	Global setting for link flapping.
`action`	Specify the action for port.
`shutdown`	Shutdown the port.

Default Linkflap action is disabled by default.

Mode Global Configuration

Example To enable the linkflap action command on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# linkflap action shutdown
```

loop-protection loop-detect

Overview Use this command to enable the loop-protection loop-detect feature and configure its parameters.

Use the **no** variant of this command to disable the loop-protection loop-detect feature.

Syntax

```
loop-protection loop-detect [ldf-interval <period>]
[ldf-rx-window <frames>] [fast-block]
```

```
no loop-protection loop-detect
```

Parameter	Description
`ldf-interval`	The time (in seconds) between successive loop-detect frames being sent.
<period>	Specify a period between 1 and 600 seconds. The default is 10 seconds.
`ldf-rx-window`	The number of transmitted loop detect frames whose details are held for comparing with frames arriving at the same port.
<frames>	Specify a value for the window size between 1 and 5 frames. The default is 3 frames.
`[fast-block]`	The fast-block blocks transmitting port to keep partial connectivity.

Default The loop-protection loop-detect feature is disabled by default. The default interval is 10 seconds, and the default window size is 3 frames.

Mode Global Configuration

Usage See the "Loop Protection" section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Example To enable the loop-detect mechanism on the switch, and generate loop-detect frames once every 5 seconds, use the following commands:

```
awplus# configure terminal
```

```
awplus(config)# loop-protection loop-detect ldf-interval 5
```

Related Commands

loop-protection action

loop-protection timeout

show loop-protection

thrash-limiting

loop-protection action

Overview Use this command to specify the protective action to apply when a network loop is detected on an interface.

Use the **no** variant of this command to reset the loop protection actions to the default action, vlan-disable, on an interface.

Syntax

```
loop-protection action
{link-down|log-only|port-disable|vlan-disable|none}
```

```
no loop-protection action
```

Parameter	Description
`link-down`	Block all traffic on a port (or aggregated link) that detected the loop, and take **down** the link.
`log-only`	Details of loop conditions are logged. No action is applied to the port (or aggregated link).
`port-disable`	Block all traffic on interface for which the loop occurred, but keep the link in the **up** state.
`vlan-disable`	Block all traffic for the VLAN on which the loop traffic was detected. Note that setting this parameter will also enable ingress filtering. This is the default action.
`none`	Applies no protective action.

Default loop-protection action vlan-disable

Mode Interface Configuration

Usage See the "Loop Protection" section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Example To disable the interface `port1.0.4` and bring the link down when a network loop is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action link-down
```

Related Commands

loop-protection loop-detect

loop-protection timeout

show loop-protection

thrash-limiting

loop-protection action-delay-time

Overview Use this command to sets the loop protection action delay time for an interface to specified values in seconds. The action delay time specifies the waiting period for the action.

Use the **no** variant of this command to reset the loop protection action delay time for an interface to default.

Syntax

```
loop-protection action-delay-time <0-86400>
no loop-protection action
```

Parameter	Description
<0-86400>	Time in seconds; 0 means action delay timer is disabled.

Default Action delay timer is disabled by default.

Mode Interface Configuration

Example To configure a loop protection action delay time of 10 seconds on port 1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection action-delay-time 10
```

Related Commands show loop-protection

loop-protection timeout

Overview Use this command to specify the Loop Protection recovery action duration on an interface.

Use the **no** variant of this command to set the loop protection timeout to the default.

Syntax

```
loop-protection timeout <duration>
no loop-protection timeout
```

Parameter	Description
<duration>	The time (in seconds) for which the configured action will apply before being disabled. This duration can be set between 0 and 86400 seconds (24 hours). The set of 0 means infinity so timeout does not expire.

Default The default is 7 seconds.

Mode Interface Configuration

Usage See the "Loop Protection" section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Example To configure a loop protection action timeout of 10 seconds for `port1.0.4`, use the command:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# loop-protection timeout 10
```

Related Commands

loop-protection loop-detect

loop-protection action

show loop-protection

thrash-limiting

mac address-table acquire

Overview Use this command to enable MAC address learning on the device.

Use the **no** variant of this command to disable learning.

Syntax
```
mac address-table acquire
no mac address-table acquire
```

Default Learning is enabled by default for all instances.

Mode Global Configuration

Example
```
awplus# configure terminal
awplus(config)# mac address-table acquire
```

mac address-table ageing-time

Overview Use this command to specify an ageing-out time for a learned MAC address. The learned MAC address will persist for at least the specified time.

The **no** variant of this command will reset the ageing-out time back to the default of 300 seconds (5 minutes).

Syntax

```
mac address-table ageing-time <ageing-timer> none
no mac address-table ageing-time
```

Parameter	Description
<ageing-timer>	*<10-1000000>* The number of seconds of persistence.
none	Disable learned MAC address timeout.

Default The default ageing time is 300 seconds.

Mode Global Configuration

Examples The following commands specify various ageing timeouts on the device:

```
awplus# configure terminal
awplus(config)# mac address-table ageing-time 1000
awplus# configure terminal
awplus(config)# mac address-table ageing-time none
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

mac address-table logging

Overview Use this command to create log entries when the content of the FDB (forwarding database) changes. Log messages are produced when a MAC address is added to or removed from the FDB.

CAUTION: *MAC address table logging may impact the performance of the switch. Only enable it when necessary as a debug tool.*

Use the **no** variant of this command to stop creating log entries when the content of the FDB changes.

Syntax

```
mac address-table logging
no mac address-table logging
```

Default MAC address table logging is disabled by default.

Mode User Exec/Privileged Exec

Usage When MAC address table logging is enabled, the switch produces the following messages:

Change	Message format	Example
MAC added	MAC add <*mac*> <*port*> <*vlan*>	MAC add eccd.6db5.68a7 port1.0.1 vlan2
MAC removed	MAC remove <*mac*> <*port*> <*vlan*>	MAC remove eccd.6db5.68a7 port1.0.1 vlan2

Note that rapid changes may not be logged. For example, if an entry is added and then removed within a few seconds, those actions may not be logged.

To see whether MAC address table logging is enabled, use the command show running-config.

Example To create log messages when the content of the FDB changes, use the command:

```
awplus# mac address-table logging
```

Related Commands show running-config

mac address-table static

Overview Use this command to statically configure the MAC address-table to forward or discard frames with a matching destination MAC address.

Syntax

```
mac address-table static <mac-addr> {forward|discard} interface
<port> [vlan <vid>]
```

```
no mac address-table static <mac-addr> {forward|discard}
interface <port> [vlan <vid>]
```

Parameter	Description
<mac-addr>	The destination MAC address in `HHHH.HHHH.HHHH` format.
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
<vid>	The VLAN ID. If you do not specify a VLAN, its value defaults to vlan 1.

Mode Global Configuration

Usage The **mac address-table static** command is only applicable to Layer 2 switched traffic within a single VLAN. Do not apply the **mac address-table static** command to Layer 3 switched traffic passing from one VLAN to another VLAN. Frames will not be discarded across VLANs because packets are routed across VLANs. This command only works on Layer 2 traffic.

Example

```
awplus# configure terminal
```

```
awplus(config)# mac address-table static 2222.2222.2222 forward
interface port1.0.4 vlan 3
```

Related Commands clear mac address-table static

show mac address-table

mac address-table thrash-limit

Overview Use this command to set the thrash limit on the device or stack.

Thrashing occurs when a MAC address table rapidly "flips" its mapping of a single MAC address between two subnets, usually as a result of a network loop.

Use the **no** variant of this command to disable thrash limiting.

Syntax

```
mac address-table thrash-limit <rate>
no mac address-table thrash-limit
```

Parameter	Description
<rate>	sets the maximum thrash rate at which limiting is applied. This rate can be set between 5 and 255 MAC thrashing flips per second. Once the thrash limit rate is reached, the port is considered to be thrashing.

Default No thrash limiting

Mode Global Configuration

Usage Use this command to limit thrashing on the selected port range.

Example To apply a thrash limit of 100 MAC address flips per second:

```
awplus# configure terminal
awplus(config)# mac address-table thrash-limit 100
```

Related Commands show mac address-table thrash-limit

mirror interface

Overview Use this command to define a mirror port and mirrored (monitored) ports and direction of traffic to be mirrored. The port for which you enter interface mode will be the mirror port.

The destination port is removed from all VLANs, and no longer participates in other switching.

Use the **no** variant of this command to disable port mirroring by the destination port on the specified source port.

Use the **none** variant of this command when using copy-to-mirror ACL and QoS commands.

Syntax

```
mirror interface <source-port-list> direction
{both|receive|transmit}
mirror interface none
no mirror interface <source-port-list>
no mirror interface none
```

Parameter	Description
<source-port-list>	The source switch ports to mirror. A port-list can be: • a port (e.g. `port1.0.2`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.2` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6` The source port list cannot include dynamic or static channel groups (link aggregators).
`direction`	Specifies whether to mirror traffic that the source port receives, transmits, or both.
`both`	Mirroring traffic both received and transmitted by the source port.
`receive`	Mirroring traffic received by the source port.
`transmit`	Mirroring traffic transmitted by the source port.
`none`	Specify this parameter for use with the ACL (Access Control List) **access-list** and QoS (Quality of Service) default action commands when used with the **copy-to-mirror** parameter option, so you can specify the destination port (the analyzer port) for the traffic without specifying a source mirror port. See the ACL commands access-list (hardware IP numbered) and access-list (hardware MAC numbered), and the QoS command default-action for further information.

Mode Interface Configuration

Usage

Use this command to send traffic to another device connected to the mirror port for monitoring.

See the "Port Mirroring" section in the Switching Feature Overview and Configuration Guide for more information.

A mirror port cannot be associated with a VLAN. If a switch port is configured to be a mirror port, it is automatically removed from any VLAN it was associated with.

This command can only be applied to a single mirror (destination) port, not to a range of ports, nor to a static or dynamic channel group. Do not apply multiple interfaces with an interface command before issuing the mirror interface command. One interface may have multiple mirror interfaces.

Example

To mirror traffic received and transmitted on `port1.0.4` and `port1.0.5` to destination `port1.0.3`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface port1.0.4,port1.0.5
direction both
```

To enable use with the access-list (hardware IP numbered) ACL and default-action QoS commands to destination `port1.0.3` without specifying a source port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# mirror interface none
```

To mirror all TCP traffic, received or transmitted to analyzer `port1.0.1`, see the sample config below:

```
awplus#show running-config

!
mls qos enable
access-list 3000 copy-to-mirror tcp any any
access-group 3000
!
interface port1.0.1
 mirror interface none
 switchport
!
```

Related Commands

access-list (hardware IP numbered)

access-list (hardware MAC numbered)

default-action

platform hwfilter-size

Overview You can use this command to control the configuration of hardware Access Control Lists (ACLs), which determines the total available number and functionality of hardware ACLs.

For this command to take effect, you need to reboot the affected service.

One cannot attach an IPv6 ACL to a port if the ACL contains a specified source or destination IPv6 address or both and the **hw-filter size** setting is **ipv4-limited-ipv6**. If you do so, a diagnostic message will be generated.

Syntax

```
platform hwfilter-size {ipv4-limited-ipv6|ipv4-full-ipv6}
```

Parameter	Description
`hwfilter-size`	Configure hardware ACLs command.
`ipv4-full-ipv6`	Configure hardware ACLs to filter IPv4 traffic, MAC addresses and IPv6 traffic, including filtering on source or destination IPv6 addresses, or both; however, this will reduce the total number of filters available in the hardware table.
`ipv4-limited-ipv6`	Configure hardware ACLs to filter IPv4 traffic, MAC addresses and IPv6 traffic. Source or destination IPv6 addresses or both are not filtered.

Default The default mode is **ipv4-limited-ipv6**.

Mode Global Configuration

Example To configure hardware ACLs to filter IPv4 and IPv6 traffic, use the following commands:

```
awplus# configure terminal
awplus(config)# platform hwfilter-size ipv4-full-ipv6
```

Related Commands show platform

ipv6 access-list (named)

platform load-balancing

Overview This command selects which address fields are used as inputs into the load balancing algorithm for aggregated links. The output from this algorithm is used to select which individual path a given packet will traverse within an aggregated link.

The **no** variant of this command turns off the specified inputs.

Syntax

```
platform load-balancing [src-dst-mac] [src-dst-ip]
[src-dest-port] [ethertype]
```

```
no platform load-balancing [src-dst-mac] [src-dst-ip]
[src-dest-port] [ethertype]
```

Parameter	Description
`src-dst-mac`	Include the source and destination MAC addresses (Layer 2)
`src-dst-ip`	Include the source and destination IP addresses (Layer 3). If you choose this option, the algorithm will use MAC addresses to calculate load balancing for Layer 2 and non-IP packets.
`src-dst-port`	The source and destination TCP/UDP port data (Layer 4). If you include this option, make sure that **src-dst-ip** is also selected.
`ethertype`	A two-octet field in an Ethernet frame that shows which protocol is encapsulated in the payload of the Ethernet frame. Ethertype is the same for all IP traffic, but is different for different kinds of non-IP traffic.

Default By default, all load-balancing input options are used.

Mode Global configuration

Usage By default, all load-balancing input options are turned on. Therefore, to use a different set of inputs, you must **turn off** the inputs you do not want.

Useful combinations of inputs include:

- all four inputs
- MAC address, IP address and Layer 4 port number
- MAC address and Ethertype
- MAC address only
- IP address and Layer 4 port number
- IP address only

The following examples show how to configure some of these combinations.

Use the show platform command to verify this command's setting.

Examples

To use all four inputs, you do not have to enter any commands, because this is the default. Note that this setting is not displayed in the **show running-config** output. Use the show platform command to verify this setting.

To use MAC addresses, IP addresses and Layer 4 port numbers, remove Ethertype by entering:

```
awplus# configure terminal
awplus(config)# no platform load-balancing ethertype
```

To use MAC addresses and Ethertype, remove the IP inputs by entering:

```
awplus# configure terminal
awplus(config)# no platform load-balancing src-dst-ip
src-dest-port
```

To use MAC addresses only, remove the other inputs by entering:

```
awplus# configure terminal
awplus(config)# no platform load-balancing src-dst-ip
src-dest-port ethertype
```

To use IP addresses and Layer 4 port numbers, remove MAC addresses and Ethertype by entering:

```
awplus# configure terminal
awplus(config)# no platform load-balancing src-dst-mac
ethertype
```

Related Commands

show platform

platform stop-unreg-mc-flooding

Overview This command stops multicast packets flooding out of all the ports in the VLAN until these packets are registered. This command does this by sending unregistered multicast packets to the switch processor, so there is no flooding of the multicast traffic onto the VLAN. Unregistered traffic will not flow until the switch has registered it, regardless of attempts to subscribe to it. Once the traffic is registered, it flows to registered subscribers and ports.

Use the **no** variant of this command to revert to default behavior and disable this feature.

NOTE: *This command should not be used within any IPv6 networks.*

IPv6 neighbor discovery operation is inhibited by this feature.

This command does not stop Local Network Control Block IPv4 multicast packets in the address range 224.0.0.1 to 224.0.0.255 (224.0.0/24).

See www.iana.org/assignments/multicast-addresses/multicast-addresses.xml#multicast-addresses-1

Syntax

```
platform stop-unreg-mc-flooding
```

no platform stop-unreg-mc-flooding

Default This feature is disabled by default.

Mode Global Configuration

Usage This command stops the periodic flooding of unknown or unregistered multicast packets when the Group Membership interval timer expires and there are no subscribers to a multicast group. If there is multicast traffic in a VLAN without subscribers, multicast traffic temporarily floods out of the VLAN when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries.

This command also stops the initial flood of multicast packets that happens when a new multicast source starts to send traffic. This flooding lasts until snooping recognizes the multicast group. For example, in sites where IP cameras have multicast groups, traffic is flooded to the VLAN and causes large bursts of traffic. Use this command when there is limited processing available for large bursts of traffic, such as in sites with IP cameras.

Output See the console message warning about IPv6 operation after entering this command:

```
% WARNING: IPv6 will not work with this setting enabled
% Please consult the documentation for more information
```

See these sample console messages when the Group Membership interval timer expires, which happens when the switch does not get replies from Group Membership queries:

```
awplus: [MLD-EVENTS] Grp - Rec Liveness Timer: Expiry for Grp ff0e::1 on port1.2.7
awplus: [IGMP-EVENTS] : Expiry (Unreg MC Timer) for Grp 224.2.2.2 on vlan4
```

Examples To enable this feature and stop multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# platform stop-unreg-mc-flooding
```

To disable this feature and allow multicast packet flooding, use the following commands:

```
awplus# configure terminal
awplus(config)# no platform stop-unreg-mc-flooding
```

Related Commands

show platform

show running-config

platform vlan-stacking-tpid

Overview This command specifies the Tag Protocol Identifier (TPID) value that applies to all frames that are carrying double tagged VLANs. All nested VLANs must use the same TPID value. (This feature is sometimes referred to as VLAN stacking or VLAN double-tagging.)

Use the **no** variant of this command to revert to the default TPID value (0x8100).

NOTE: *Because the additional tag increases the frame size beyond 1522 bytes, you must increase the MRU size to activate VLAN-stacking. Go into interface mode for the appropriate ports and use the mru command.*

Syntax

```
platform vlan-stacking-tpid <tpid>
no platform vlan-stacking-tpid
```

Parameter	Description
<tpid>	The Ethernet type of the tagged packet, as a two byte hexadecimal number.

Default The default TPID value is 0x8100.

Mode Global Configuration

Examples To set the VLAN stacking TPID value to 0x9100, use the following commands:

```
awplus# configure terminal
awplus(config)# platform vlan-stacking-tpid 9100
```

To reset the VLAN stacking TPID value to the default (0x8100), use the following commands:

```
awplus# configure terminal
awplus(config)# no platform vlan-stacking-tpid
```

Related Commands switchport vlan-stacking (double tagging)

show platform

show running-config

polarity

Overview This command sets the MDI/MDIX polarity on a copper-based switch port.

Syntax

```
polarity {auto|mdi|mdix}
```

Parameter	Description
`mdi`	Sets the polarity to MDI (medium dependent interface).
`mdix`	Sets the polarity to MDI-X (medium dependent interface crossover).
`auto`	The switch port sets the polarity automatically. This is the default option.

Default By default, switch ports set the polarity automatically (**auto**).

Mode Interface Configuration

Usage We recommend the default **auto** setting for MDI/MDIX polarity. Polarity applies to copper 10BASE-T, 100BASE-T, and 1000BASE-T switch ports; It does not apply to fiber ports. See the "MDI/MDIX Connection Modes" section in the Switching Feature Overview and Configuration Guide for more information.

Example To set the polarity for `port1.0.6` to fixed MDI mode, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# polarity mdi
```

show debugging loopprot

Overview This command shows Loop Protection debugging information.

Syntax

```
show debugging loopprot
```

Mode User Exec and Privileged Exec

Example To display the enabled Loop Protection debugging modes, use the command:

```
awplus# show debugging loopprot
```

Related Commands debug loopprot

show debugging platform packet

Overview This command shows platform to CPU level packet debugging information.

Syntax
```
show debugging platform packet
```

Mode User Exec and Privileged Exec

Example To display the platform packet debugging information, use the command:

```
awplus# show debugging platform packet
```

Related Commands debug platform packet

undebug platform packet

show flowcontrol interface

Overview Use this command to display flow control information.

Syntax

```
show flowcontrol interface <port>
```

Parameter	Description
<port>	Specifies the name of the port to be displayed.

Mode User Exec and Privileged Exec

Example To display the flow control for the `port1.0.5`, use the command:

```
awplus# show flowcontrol interface port1.0.5
```

Output Figure 12-1: Example output from the **show flowcontrol interface** command for a specific interface

```
Port     Send  FlowControl    Receive  FlowControl  RxPause TxPause
          admin    oper         admin    oper
-----      ------- --------     ------- --------     ------- -------
port1.0.5 on       on           on       on           0       0
```

show interface err-disabled

Overview Use this command to show the ports which have been dynamically shut down by protocols running on the device and the protocols responsible for the shutdown.

Syntax

```
show interface [<IFRANGE> err-disabled]
```

Parameter	Description
<IFRANGE>	Interface range
`err-disabled`	Brief summary of interfaces shut down by protocols

Mode User Exec and Privileged Exec

Example Show the protocols that have shut down port2.0.21 and port2.0.23, use the commands:

```
awplus# show interface err-disabled
```

Output Figure 12-2: Example output from the **show interface err-disabled** command

```
awplus#show interface err-disabled
Interface            Reason
port2.0.21           loop protection
port2.0.23           loop protection
```

show interface switchport

Overview Use this command to show VLAN information about each switch port.

Syntax

```
show interface switchport
```

Mode User Exec and Privileged Exec

Example To display VLAN information about each switch port, enter the command:

```
awplus# show interface switchport
```

Output Figure 12-3: Example output from the **show interface switchport** command

```
 Interface name          : port1.0.1
 Switchport mode         : access
 Ingress filter          : enable
 Acceptable frame types  : all
 Default Vlan            :  2
 Configured Vlans        : 2

 Interface name          : port1.0.2
 Switchport mode         : trunk
 Ingress filter          : enable
 Acceptable frame types  : all
 Default Vlan            :  1
 Configured Vlans        : 1 4 5 6 7 8
...
```

Related Commands show interface memory

show loop-protection

Overview Use this command to display the current loop protection setup for the device.

Syntax `show loop-protection [interface <port-list>] [counters]`

Parameter	Description
`interface`	The interface selected for display.
`<port-list>`	A port, a port range, or an aggregated link.
`counters`	Displays counter information for loop protection.

Mode User Exec and Privileged Exec

Usage This command is used to display the current configuration and operation of the Loop Protection feature

Examples To display the current configuration status for `port1.0.1`, use the command:

```
awplus# show loop-protection interface port1.0.1
```

Figure 12-4: Example output from the **show loop-protection** command

```
Loop-Detection:          Enabled
LDF Interval:            10 [sec]
Interface:               port1.0.1
 Action:                 port-disable
 Timeout:                300 [sec]
 Vlan:                   1
  Status:                Blocking
  Timeout Remaining:     115 [sec]
 Vlan:                   2
  Status:                Normal
  Timeout Remaining:     0 [sec]
```

To display the counter information for `port1.0.1`, use the command:

```
awplus# show loop-protection interface port1.0.1 counters
```

Figure 12-5: Example output from the **show loop-protection interface counters** command for port1.0.1

```
Interface:              port1.0.1
 Vlan:                  1
  LDF Tx:               3
  LDF Rx:               1
  Invalid LDF Rx:       1
  Action:               1
Vlan:                   2
  LDF Tx:               3
  LDF Rx:               0
  Invalid LDF Rx:       0
  Action:               0
```

show mac address-table

Overview Use this command to display the mac address-table for all configured VLANs.

Syntax

```
show mac address-table
```

Mode User Exec and Privileged Exec

Usage The **show mac address-table** command is only applicable to view a mac address-table for Layer 2 switched traffic within VLANs.

Example To display the mac address-table, use the following command:

```
awplus# show mac address-table
```

Output See the below sample output captured when there was no traffic being switched:

```
awplus#show mac address-table

VLAN Port          MAC               State
1    unknown       0000.cd28.0752    static
ARP  -             0000.cd00.0000    static
```

See the sample output captured when packets were switched and mac addresses were learned:

```
awplus#show mac address-table

VLAN Port          MAC               State
1    unknown       0000.cd28.0752    static
1    port1.0.6     0030.846e.9bf4    dynamic
1    port1.0.4     0030.846e.bac7    dynamic
ARP  -             0000.cd00.0000    static
```

Note the new mac addresses learned for `port1.0.4` and `port1.0.6` added as dynamic entries.

Note the first column of the output below shows VLAN IDs if multiple VLANs are configured:

```
awplus#show mac address-table

VLAN Port          MAC               State
1    unknown       0000.cd28.0752    static
1    port1.0.4     0030.846e.bac7    dynamic
2    unknown       0000.cd28.0752    static
2    port1.0.6     0030.846e.9bf4    dynamic
ARP  -             0000.cd00.0000    static
```

Also note manually configured static mac-addresses are shown to the right of the type column:

```
awplus(config)#mac address-table static 0000.1111.2222 for int
port1.0.3 vlan 2
awplus(config)#end
awplus#
awplus#show mac address-table

VLAN Port          MAC               State
1    unknown       0000.cd28.0752    static
1    port1.0.2     0030.846e.bac7    dynamic
2    port1.0.3     0000.1111.2222    static
2    unknown       0000.cd28.0752    static
2    port1.0.5     0030.846e.9bf4    dynamic
ARP  -             0000.cd00.0000    statics
```

Related Commands

clear mac address-table dynamic

clear mac address-table static

mac address-table static

show mac address-table thrash-limit

Overview Use this command to display the current thrash limit set for all interfaces on the device.

Syntax

```
show mac address-table thrash-limit
```

Mode User Exec and Privileged Exec

Example To display the current, use the following command:

```
awplus# show mac address-table thrash-limit
```

Output Figure 12-6: Example output from the **show mac address-table thrash-limit** command

```
% Thrash-limit  7 movements per second
```

Related Commands mac address-table thrash-limit

show mirror

Overview Use this command to display the status of all mirrored ports.

Syntax

```
show mirror
```

Mode User Exec and Privileged Exec

Example To display the status of all mirrored ports, use the following command:

```
awplus# show mirror
```

Output Figure 12-7: Example output from the **show mirror** command

```
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.2
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.4
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.1
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: receive
Monitored Port Name: port1.0.3
Mirror Test Port Name: port1.0.1
Mirror option: Enabled
Mirror direction: transmit
Monitored Port Name: port1.0.4
```

show mirror interface

Overview Use this command to display port mirroring configuration for a mirrored (monitored) switch port.

Syntax

```
show mirror interface <port>
```

Parameter	Description
<port>	The monitored switch port to display information about.

Mode User Exec, Privileged Exec and Interface Configuration

Example To display port mirroring configuration for the `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# show mirror interface port1.0.4
```

Output Figure 12-8: Example output from the **show mirror interface** command

```
Mirror Test Port Name: port1.0.3
Mirror option: Enabled
Mirror direction: both
Monitored Port Name: port1.0.4
```

show platform

Overview This command displays the settings configured by using the **platform** commands.

Syntax

```
show platform
```

Mode Privileged Exec

Usage This command displays the settings in the running config. For changes in some of these settings to take effect, the device must be rebooted with the new settings in the startup config.

Example To check the settings configured with **platform** commands on the device, use the following command:

```
awplus# show platform
```

Output Figure 12-9: Example output from the **show platform** command

```
awplus# show platform

Vlan-stacking TPID           0x8100
```

Table 5: Parameters in the output of the **show platform** command

Parameter	Description
Load Balancing	
Vlan-stacking TPID	The value of the TPID set in the Ethernet type field when a frame has a double VLAN tag (platform vlan-stacking-tpid command).

Related Commands

platform load-balancing

platform vlan-stacking-tpid

show platform classifier statistics utilization brief

Overview This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

Syntax

```
show platform classifier statistics utilization brief
```

Mode Privileged Exec

Example To display the platform classifier utilization statistics, use the following command:

```
awplus# show platform classifier statistics utilization brief
```

Output Figure 12-10: Output from the **show platform classifier statistics utilization brief** command

```
awplus#show platform classifier statistics utilization brief

[Instance 0]
  Number of Entries:
  Policy Type      Group ID   Used / Total
  ---------------------------------------------
  ACL              1476395009    0 /  118 (  0%)
  Web Auth         Inactive      0 /    0 (  0%)
  QoS                            0 /  128 (  0%)
```

Related Commands show platform

show platform port

Overview This command displays the various port registers or platform counters for specified switchports.

Syntax

```
show platform port [<port-list>|counters]
```

Parameter	Description
<port-list>	The ports to display information about. A port-list can be: • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.6` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`.
`counters`	Show the platform counters.

Mode Privileged Exec

Examples To display port registers for `port1.0.1` and `port1.0.2` use the following command:

```
awplus# show platform port port1.0.1-port1.0.2
```

To display platform counters for `port1.0.1` and `port1.0.2` use the following command:

```
awplus# show platform port port1.0.1-port1.0.2 counters
```

Output Figure 12-11: Example output from the **show platform port** command

```
awplus#show platform port port1.0.1
Phy register value for port1.0.1 (ifindex: 5001)

00:1140  01:79ed  02:0362  03:5e7b  04:01e1  05:c1e1  06:006d  07:2001
08:4d77  09:0600  0a:3800  0b:0000  0c:0000  0d:4007  0e:0000  0f:3000
10:0000  11:0f00  12:0000  13:0400  14:0000  15:0000  16:0000  17:0000
18:4400  19:871c  1a:243e  1b:ffff  1c:0000  1d:2442  1e:0000  1f:0000


Port configuration for lport 0x08002003:
Phy Driver: 54680 Gigabit PHY Driver
  enabled:                1
  loopback:               0
  link:                   1
  speed:               1000  max speed:              1000
  duplex:                 1
  linkscan:               2
  autonegotiate:          1
  master:                 2
  tx pause:               0  rx pause:                  0
  untagged vlan:       4000
  vlan filter:            3
  stp state:              4
  learn:                  5
  discard:                0
  jam:                    0
  max frame size:      1500
  MC Disable SA:         no
  MC Disable TTL:        no
  MC egress untag:        0
  MC egress vid:          1
  MC TTL threshold:      -1
```

Table 6: Parameters in the output from the **show platform port** command

Parameter	Description
Ethernet MAC counters	
Combined receive/ transmit packets by size (octets) counters	Number of packets in each size range received and transmitted.
64	Number of 64 octet packets received and transmitted.
65 - 127	Number of 65 - 127 octet packets received and transmitted.
128 - 255	Number of 128 - 255 octet packets received and transmitted.

Table 6: Parameters in the output from the **show platform port** command

Parameter	Description
256 - 511	Number of 256 - 511 octet packets received and transmitted.
512 - 1023	Number of 512 - 1023 octet packets received and transmitted.
1024 - MaxPktSz	Number of packets received and transmitted with size 1024 octets to the maximum packet length.
1519 - 1522	Number of 1519 - 1522 octet packets received and transmitted.
1519 - 2047	Number of 1519 - 2047 octet packets received and transmitted.
2048 - 4095	Number of 2048 - 4095 octet packets received and transmitted.
4096 - 9216	Number of 4096 - 9216 octet packets received and transmitted.
General Counters	
Receive	Counters for traffic received.
Octets	Number of octets received.
Pkts	Number of packets received.
FCSErrors	Number of FCS (Frame Check Sequence) error events received.
UnicastPkts	Number of unicast packets received.
MulticastPkts	Number of multicast packets received.
BroadcastPkts	Number of broadcast packets received.
PauseMACCtlFrms	Number of Pause MAC Control Frames received.
OversizePkts	Number of oversize packets received.
Fragments	Number of fragments received.
Jabbers	Number of jabber frames received.
UnsupportOpcode	Number of MAC Control frames with unsupported opcode received.
AlignmentErrors	Receive Alignment Error Frame Counter.
SysErDurCarrier	Receive Code Error Counter.

Table 6: Parameters in the output from the **show platform port** command

Parameter	Description
CarrierSenseErr	Receive False Carrier Counter.
UndersizePkts	Number of undersized packets received.
Transmit	Counters for traffic transmitted.
Octets	Number of octets transmitted.
Pkts	Number of packets transmitted.
UnicastPkts	Number of unicast packets transmitted.
MulticastPkts	Number of multicast packets transmitted.
BroadcastPkts	Number of broadcast packets transmitted.
PauseMACCtlFrms	Number of Pause MAC Control Frames transmitted.
OversizePkts	Number of oversize packets transmitted.
FrameWDeferrdTx	Transmit Single Deferral Frame counter.
FrmWExcesDefer	Transmit Multiple Deferral Frame counter.
SingleCollsnFrm	Transmit Single Collision Frame counter.
MultCollsnFrm	Transmit Multiple Collision Frame counter.
LateCollisions	Transmit Late Collision Frame counter.
ExcessivCollsns	Transmit Excessive Collision Frame counter.
Collisions	Transmit Total Collision counter
Layer 3 Counters	
ifInUcastPkts	Inbound interface Unicast counter.
ifInDiscards	Inbound interface Discarded Packets counter.
ipInHdrErrors	Inbound interface Header Errors counter.
ifOutUcastPkts	Outbound interface Unicast counter.
ifOutErrors	Outbound interface Error counter.
Miscellaneous Counters	
DropEvents	Drop Event counter
ifOutDiscards	Outbound interface Discarded Packets counter.
MTUExcdDiscard	Receive MTU Check Error Frame Counter

show port-security interface

Overview Use this command to show the current port-security configuration and the switch port status.

Syntax

```
show port-security interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).

Mode Privileged Exec

Example To see the port-security status on port1.0.1, use the following command:

```
awplus# show port-security interface port1.0.1
```

Output Figure 12-12: Example output from the **show port-security interface** command

```
Port Security configuration
Security Enabled              : YES
Port Status                   : ENABLED
Violation Mode                : TRAP
Aging                         : OFF
Maximum MAC Addresses         : 3
Total MAC ddresses            : 1
Lock Status                   : UNLOCKED
Security Violation Count      : 0
Last Violation Source Address : None
```

Related Commands

clear port-security intrusion

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security maximum

switchport port-security violation

show port-security intrusion

Overview Use this command to show the intrusion list. If the port is not specified, the entire intrusion table is shown.

Syntax

```
show port-security intrusion [interface <port>]
```

Parameter	Description
`interface`	Specify a port
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).

Mode Privileged Exec

Example To see the intrusion list on `port1.0.1`, use the following command:

```
awplus# show port-security intrusion interface port1.0.1
```

Output Figure 12-13: Example output from the **show port-security intrusion** command for port 1.0.1

```
Port Security Intrusion List
Interface: port1.0.1 -3 intrusion(s) detected
11-22-33-44-55-04 11-22-33-44-55-06 11-22-33-44-55-08
```

Related Commands

clear port-security intrusion

show port-security interface

switchport port-security

switchport port-security aging

switchport port-security maximum

switchport port-security violation

show storm-control

Overview Use this command to display storm-control information for all interfaces or a particular interface.

Syntax

```
show storm-control [<port>]
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec and Privileged Exec

Example To display storm-control information for `port1.0.2`, use the following command:

```
awplus# show storm-control port1.0.2
```

Output Figure 12-14: Example output from the **show storm-contro**l command for port1.0.2

```
Port       BcastLevel  McastLevel  DlfLevel
port1.0.2      40. 0%     100. 0%   100. 0%
```

Related Commands storm-control level

speed

Overview This command changes the speed of the specified port. You can optionally specify the speed or speeds that get autonegotiated, so autonegotiation is only attempted at the specified speeds.

To see the currently-negotiated speed for ports whose links are up, use the show interface command. To see the configured speed (when different from the default), use the show running-config command.

Syntax

```
speed {10|100|1000|10000|auto [10][100][1000][10000]}
```

The following table shows the speed options for each type of port.

Port type	Speed Options (units are Mbps)
RJ-45 and RJ.5copper ports	auto (default) 10 100 1000
10000Mbps fiber SFP+	auto (default) 10000

Mode Interface Configuration

Default By default, ports autonegotiate speed.

Usage Switch ports in a static or dynamic (LACP) channel group must have the same port speed and be in full duplex mode. Once switch ports have been aggregated into a channel group, you can set the speed of all the switch ports in the channel group by applying this command to the channel group.

NOTE: *If multiple speeds are specified after the auto option to autonegotiate speeds, then the device only attempts autonegotiation at those specified speeds.*

Examples To set the speed of a tri-speed port to 100Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed 100
```

To return the port to auto-negotiating its speed, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto
```

To set the port to auto-negotiate its speed at 100Mbps and 1000Mbps, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 100 1000
```

To set the port to auto-negotiate its speed at 1000Mbps only, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# speed auto 1000
```

Related Commands

duplex

ecofriendly lpi

polarity

show interface

speed (asyn)

storm-control level

Overview Use this command to specify the speed limiting level for broadcasting, multicast, or destination lookup failure (DLF) traffic for the port. Storm-control limits the selected traffic type to the specified percentage of the maximum port speed.

Use the **no** variant of this command to disable storm-control for broadcast, multicast or DLF traffic.

Syntax

```
storm-control {broadcast|multicast|dlf} level <level>
no storm-control {broadcast|multicast|dlf} level
```

Parameter	Description
<level>	<0-100> Specifies the percentage of the maximum port speed allowed for broadcast, multicast or destination lookup failure traffic.
broadcast	Applies the storm-control to broadcast frames.
multicast	Applies the storm-control to multicast frames.
dlf	Applies the storm-control to destination lookup failure traffic.

Default By default, storm-control is disabled.

Mode Interface Configuration

Usage Flooding techniques are used to block the forwarding of unnecessary flooded traffic. A packet storm occurs when a large number of broadcast packets are received on a port. Forwarding these packets can cause the network to slow down or time out.

Example To limit broadcast traffic on `port1.0.2` to 30% of the maximum port speed, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# storm-control broadcast level 30
```

Related Commands show storm-control

switchport port-security

Overview Use this command to enable the port-security feature. This feature is also known as the port-based learn limit. It allows the user to set the maximum number of MAC addresses that each port can learn.

Use the **no** variant of this command to disable the port-security feature.

Syntax

```
switchport port-security
no switchport port-security
```

Mode Interface Configuration

Examples To enable the port-security feature on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security
```

To disable the port-security feature on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security
```

Related Commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security aging

switchport port-security maximum

switchport port-security violation

switchport port-security aging

Overview Use this command to set MAC addresses that have been learned by port security to age out.

Use the **no** variant of this command to set the MAC addresses to not age out.

Syntax

```
switchport port-security aging
no switchport port-security aging
```

Mode Interface Configuration

Examples To set port1.0.4 so that the MAC addresses that have been learned by port security age out, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security aging
```

To stop the MAC addresses that have been learned by port security from aging out on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security aging
```

Related Commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security maximum

switchport port-security violation

switchport port-security maximum

Overview Use this command to set the maximum number of MAC addresses that each port can learn.

Use the **no** variant of this command to unset the maximum number of MAC addresses that each port can learn. This is same as setting the maximum number to 0. This command also resets the intrusion list table.

If a new MAC is seen on a port with port security enabled and the MAC is statically configured for another port, a violation is triggered. The maximum learn limit will be ignored and the specified intrusion action for the port will be carried out.

Syntax

```
switchport port-security maximum <0-256>
no switchport port-security maximum
```

Parameter	Description
`maximum <0-256>`	Specify the maximum number of addresses to learn.

Mode Interface Configuration

Examples To learn 3 MAC addresses on `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security maximum 3
```

To remove the MAC learning limit on `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security maximum
```

Related Commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security violation

switchport port-security violation

Overview Use this command to set the action taken on a switch port when the port exceeds the learning limits. The port action can be either **shutdown**, **restrict** or **protect**. If **shutdown** is set, the physical link will be disabled and "shutdown" will be shown in the config. If **restrict** is set, the packet from the un-authorized MAC will be discarded and SNMP TRAP will be generated to alert management. If **protect** is set, the packet will simply be discarded by the packet processor silently.

Use the **no** variant of this command to set the violation action to default. The default violation action is protect.

Syntax

```
switchport port-security violation {shutdown|restrict|protect}
no switchport port-security violation
```

Parameter	Description
`shutdown`	Disable the port.
`restrict`	Alert the network administrator.
`protect`	Discard the packet.

Mode Interface Configuration

Examples To set the action to be shutdown on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# switchport port-security violation shutdown
```

To set the port-security action to the default (protect) on port1.0.4, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport port-security violation
```

Related Commands

clear port-security intrusion

show port-security interface

show port-security intrusion

switchport port-security

switchport port-security aging

switchport port-security maximum

thrash-limiting

Overview Sets and configures the thrash limit action that will be applied to any port on the device when a thrashing condition is detected. The thrash-limiting timeout specifies the time, in seconds, for which the thrash action is employed.

Syntax

```
thrash-limiting {[action
{learn-disable|link-down|port-disable|vlan-disable|none}]
[timeout <0-86400>]}
```

```
no thrash-limiting {action|timeout}
```

Parameter	Description
`action`	The mac thrashing detected action. The default is vlan-disable.
`learn-disable`	Disable mac address learning
`link-down`	Block all traffic on an interface - link down
`port-disable`	Block all traffic on an interface - link remains up
`vlan-disable`	Block all traffic on a vlan. Note that setting this parameter will also enable ingress filtering.
`none`	No thrash action
`timeout`	Set the duration for the thrash action
<0-86400>	The duration of the applied thrash action in seconds. The default is 1 seconds.

Default The default action is learn-disable.

Mode Interface Configuration

Usage See the "Thrash Limiting" section in the Switching Feature Overview and Configuration Guide for relevant conceptual, configuration, and overview information prior to applying this command.

Examples To set the action to learn disable for `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# thrash-limiting action learn-disable
```

To block all traffic on a vlan, use the following command:

```
awplus# configure terminal
awplus(config)# thrash-limiting action vlan-disable
```

To set the thrash limiting timeout to 5 seconds, use the following command:

```
awplus(config-if)# thrash-limiting timeout 5
```

To set the thrash limiting action to its default, use the following command:

```
awplus(config-if)# no thrash-limiting action
```

To set the thrash limiting timeout to its default, use the following command:

```
awplus(config-if)# no thrash-limiting timeout
```

Related Commands

loop-protection loop-detect

loop-protection action

loop-protection timeout

show loop-protection

undebug loopprot

Overview This command applies the functionality of the no debug loopprot command.

undebug platform packet

Overview This command applies the functionality of the no debug platform packet command.

13 VLAN Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure VLANs. For more information see the VLAN Feature Overview and Configuration Guide.

Command List

clear vlan statistics

Overview This command resets the counters for either a specific VLAN statistics instance or (by not specifying an instance) resets the counters for all instances.

The terms **frame** and **packet** are used interchangeably.

Syntax

```
clear vlan statistics [name <instance_name>]
```

Parameter	Description
`vlan statistics`	The count of incoming frames or bytes collected on a per VLAN basis.[1]
`<instance-name>`	The name of the instance for which incoming frames and their bytes are counted.[1]

Mode Privileged Exec

Examples To reset all packet counters for the packet counter instance **vlan2-data:**

```
awplus# clear vlan statistics name vlan2-data
```

To reset all packet counters for all packet counter instances.

```
awplus# clear vlan statistics
```

Related Commands show vlan statistics

vlan statistics

port-vlan-forwarding-priority

Overview Use this command to set the highest priority protocol to control transitions from blocking to forwarding traffic. This command prioritizes switch port forwarding mode control, when more than one of EPSR, Loop Protection, and MAC thrashing protection protocols are used on the switch.

EPSR, Loop Protection and MAC Thrashing use the same mechanism to block or forward traffic. This command sets the highest priority protocol to control transitions from blocking to forwarding traffic. Setting the priority stops contention between protocols.

For example, If EPSR is set to the highest priority protocol to block traffic on vlan10 on port1.0.2 then this stops MAC Thrashing from forwarding traffic on vlan10 on port1.0.2.

CAUTION: *The **loop-protection** and **none** parameter options must not be set on an EPSR master node. Use the epsr parameter option on an EPSR master node instead. Setting this command incorrectly on an EPSR master node could cause unexpected broadcast storms* **.**

Use the **no** variant of this command to restore the default highest priority protocol back to the default of EPSR.

For more information about EPSR, see the EPSR Feature Overview and Configuration Guide.

Syntax

```
port-vlan-forwarding-priority {epsr|loop-protection|none}
no port-vlan-forwarding-priority
```

Parameter	Description
`epsr`	Sets EPSR as the highest priority protocol. Use this parameter on an EPSR master node to avoid unexpected broadcast storms.
`loop-protection`	Sets Loop Protection as the highest priority protocol. Note that this option must not be set on an EPSR master node. Use the epsr parameter option on an EPSR master node to avoid unexpected broadcast storms.
`none`	Sets the protocols to have equal priority. This was the previous behavior before this command was added, and allows protocols to override each other to set a port to forwarding a VLAN. Note that this option must not be set on a EPSR master node. Use the epsr parameter option on an EPSR master node to avoid unexpected broadcast storms.

Default By default, the highest priority protocol is EPSR

Mode Global Configuration

Usage EPSR, Loop Protection and MAC Thrashing protection do not usually need to be configured on a switch, because they perform similar functions—each prevents network loops by blocking a selected port for each (loop containing) VLAN.

However, if more than one of these three features is configured on a switch, you can use this command to prioritize either EPSR or Loop Protection when their effects on a port would conflict and override each other. Previously, each protocol could set a port to forwarding for a VLAN, sometimes overriding the previous setting by another protocol to block the port. This could sometimes lead to unexpected broadcast storms.

Now, when a protocol is set to have the highest priority over a data VLAN on a port, it will not allow other protocols to put that port-vlan into a forwarding state if the highest priority protocol blocked it.

The priority mechanism is only used for blocking-to-forwarding transitions; protocols remain independent on the forwarding-to-blocking transitions.

For example, with an EPSR master node in a two-node ESPR ring with the below settings:

- The EPSR master node primary port is configured to switchport interface port1.0.1
- The EPSR master node secondary port is configured to switchport interface port1.0.2
- The EPSR master node control VLAN is configured to VLAN interface vlan10
- The EPSR master node has a first data VLAN configured to VLAN interface vlan20
- The EPSR master node has a second data VLAN configured to VLAN interface vlan30.

Initially, the EPSR ring is complete, with port1.0.2 blocking data VLANs vlan20 and vlan30 and some broadcast traffic flowing through. If the user removes vlan30 from EPSR, a storm is created on vlan30. MAC thrashing protection detects it and blocks vlan30.

Then after the storm has stopped, MAC thrashing protection sets it to forwarding again and it keeps oscillating between forwarding and blocking. In the meantime, the user adds back vlan30 to EPSR as a data VLAN and EPSR blocks it on port1.0.2.

If the priority is set to none (**port-vlan-forwarding-priority none**), MAC thrashing protection notices that the storm has stopped again and decides to put vlan30 on port1.0.2 into forwarding state. This overrides what EPSR requires for this port-VLAN and creates a storm. This matches the old behavior before this feature was implemented.

If the priority is set to EPSR or default (**port-vlan-forwarding-priority epsr**), MAC thrashing protection notices that the storm has stopped again and attempts to put vlan30 on port1.0.2 into forwarding state. The higher priority protocol (EPSR) is blocking the VLAN on this port, so it stays blocking and no storm occurs.

Example

To prioritize EPSR over Loop Protection or MAC Thrashing protection settings, so that Loop Protection or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if EPSR has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority epsr
```

To prioritize Loop Protection over EPSR or MAC Thrashing protection settings, so that EPSR or MAC Thrashing protection cannot set a port to the forwarding state a VLAN if Loop Protection has set it to the blocking state, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority loop-protection
```

To set EPSR, Loop Protection, and MAC Thrashing protection protocols to have equal priority for port forwarding and blocking, which allows the protocols to override each other to set a port to the forwarding or blocking states, use the commands:

```
awplus# configure terminal
awplus(config)# port-vlan-forwarding-priority none
```

To restore the default highest priority protocol back to the default of EPSR, use the commands:

```
awplus# configure terminal
awplus(config)# no port-vlan-forwarding-priority
```

Related Commands

show port-vlan-forwarding-priority

private-vlan

Overview Use this command to a create a private VLAN. Private VLANs can be either primary or secondary. Secondary VLANs can be ether community or isolated.

Use the **no** variant of this command to remove the specified private VLAN.

For more information, see the VLAN Feature Overview and Configuration Guide.

Syntax

```
private-vlan <vlan-id> {community|isolated|primary}
no private-vlan <vlan-id> {community|isolated|primary}
```

Parameter	Description
<vlan-id>	VLAN ID in the range <2-4094> for the VLAN which is to be made a private VLAN.
community	Community VLAN.
isolated	Isolated VLAN.
primary	Primary VLAN.

Mode VLAN Configuration

Examples

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2 name vlan2 state enable
awplus(config-vlan)# vlan 3 name vlan3 state enable
awplus(config-vlan)# vlan 4 name vlan4 state enable
awplus(config-vlan)# private-vlan 2 primary
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 community
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 primary
awplus(config-vlan)# no private-vlan 3 isolated
awplus(config-vlan)# no private-vlan 4 community
```

private-vlan association

Overview Use this command to associate a secondary VLAN to a primary VLAN. Only one isolated VLAN can be associated to a primary VLAN. Multiple community VLANs can be associated to a primary VLAN.

Use the **no** variant of this command to remove association of all the secondary VLANs to a primary VLAN.

For more information, see the VLAN Feature Overview and Configuration Guide.

Syntax

```
private-vlan <primary-vlan-id> association {add
<secondary-vlan-id>|remove <secondary-vlan-id>}
```

```
no private-vlan <primary-vlan-id> association
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vlan-id>	VLAN ID of the secondary VLAN (either isolated or community).

Mode VLAN Configuration

Examples The following commands associate primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association add 3
```

The following commands remove the association of primary VLAN 2 with secondary VLAN 3:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# private-vlan 2 association remove 3
```

The following commands remove all secondary VLAN associations of primary VLAN 2:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no private-vlan 2 association
```

show port-vlan-forwarding-priority

Overview Use this command to display the highest priority protocol that controls port-vlan forwarding or blocking traffic. This command displays whether EPSR or Loop Protection is set as the highest priority for determining whether a port forwards a VLAN, as set by the port-vlan-forwarding-priority command.

For more information about EPSR, see the EPSR Feature Overview and Configuration Guide.

Syntax

```
show port-vlan-forwarding-priority
```

Mode Privileged Exec

Example To display the highest priority protocol, use the command:

```
awplus# show port-vlan-forwarding-priority
```

Output Figure 13-1: Example output from the **show port-vlan-forwarding-priority** command

```
Port-vlan Forwarding Priority: EPSR
```

Related Commands port-vlan-forwarding-priority

show interface switchport vlan translation

Overview Use this command to display VLAN translation information for some or all interfaces.

Syntax

```
show interface switchport vlan translation interface [<int>]
```

Parameter	Description
`interface <int>`	The interface to display information about. An interface can be a switch port (e.g. port1.0.6), a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2).

Mode User Exec/Privileged Exec

Example To display VLAN translation information for port1.0.1, use the command:

```
awplus# show interface switchport vlan translation port1.0.1
```

Output Figure 13-2: Example output from **show interface switchport vlan translation port1.0.1**

```
awplus#show interface switchport vlan translation port1.0.1

Interface: port1.0.1
VLAN on Wire    VLAN
-------------   ---------------
  1649          100
  default       drop
```

Table 13-1: Parameters in the output from **show interface switchport vlan translation**

Parameter	Description
Interface	The interface on which VLAN-IDs will be translated
VLAN on Wire	VLAN-ID of the packet as it will be seen on the wire
VLAN	VLAN-ID of the VLAN as it was assignedwhen the VLAN was created
default	The action taken on inbound tagged packets that do not match a VLAN translation entry; either **drop** or **accept**

Related Commands switchport vlan translation

switchport vlan translation default drop

show vlan

Overview Use this command to display information about a particular VLAN by specifying its VLAN ID. Selecting **all** will display information for all the VLANs configured.

Syntax `show vlan {all|brief|dynamic|static|auto|static-ports<1-4094>}`

Parameter	Description
<1-4094>	Display information about the VLAN specified by the VLAN ID.
`all`	Display information about all VLANs on the device.
`brief`	Display information about all VLANs on the device.
`dynamic`	Display information about all VLANs learned dynamically.
`static`	Display information about all statically configured VLANs.
`auto`	Display information about all auto-configured VLANs.
`static- ports`	Display static egress/forbidden ports.

Mode User Exec and Privileged Exec

Example To display information about VLAN 2, use the command:

```
awplus# show vlan 2
```

Output Figure 13-3: Example output from the **show vlan** command

```
VLAN ID  Name            Type    State   Member ports
                                         (u)-Untagged, (t)-Tagged
======= ================ ======= ======= ====================================
2       VLAN0002         STATIC  ACTIVE  port1.0.3(u) port1.0.4(u) port1.0.5(u)
                                         port1.0.6(u)
...
```

Related Commands vlan

show vlan classifier group

Overview Use this command to display information about all configured VLAN classifier groups or a specific group.

Syntax

```
show vlan classifier group [<1-16>]
```

Parameter	Description
<1-16>	VLAN classifier group identifier

Mode User Exec and Privileged Exec

Usage If a group ID is not specified, all configured VLAN classifier groups are shown. If a group ID is specified, a specific configured VLAN classifier group is shown.

Example To display information about VLAN classifier group 1, enter the command:

```
awplus# show vlan classifier group 1
```

Related Commands vlan classifier group

show vlan classifier group interface

Overview Use this command to display information about a single switch port interface for all configured VLAN classifier groups.

Syntax

```
show vlan classifier group interface <switch-port>
```

Parameter	Description
<switch-port>	Specify the switch port interface classifier group identifier

Mode User Exec and Privileged Exec

Usage All configured VLAN classifier groups are shown for a single interface.

Example To display VLAN classifier group information for switch port interface `port1.0.2`, enter the command:

```
awplus# show vlan classifier group interface port1.0.2
```

Output Figure 13-4: Example output from the **show vlan classifier group interface port1.0.1** command:

```
vlan classifier group 1 interface port1.0.1
```

Related Commands

vlan classifier group

show vlan classifier interface group

show vlan classifier interface group

Overview Use this command to display information about all interfaces configured for a VLAN group or all the groups.

Syntax

```
show vlan classifier interface group [<1-16>]
```

Parameter	Description
<1-16>	VLAN classifier interface group identifier

Mode User Exec and Privileged Exec

Usage If a group ID is not specified, all interfaces configured for all VLAN classifier groups are shown. If a group ID is specified, the interfaces configured for this VLAN classifier group are shown.

Example To display information about all interfaces configured for all VLAN groups, enter the command:

```
awplus# show vlan classifier interface group
```

To display information about all interfaces configured for VLAN group 1, enter the command:

```
awplus# show vlan classifier interface group 1
```

Output Figure 13-5: Example output from the **show vlan classifier interface group** command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
vlan classifier group 2 interface port1.0.3
vlan classifier group 2 interface port1.0.4
```

Output Figure 13-6: Example output from the **show vlan classifier interface group** 1 command

```
vlan classifier group 1 interface port1.0.1
vlan classifier group 1 interface port1.0.2
```

Related Commands vlan classifier group

show vlan classifier group interface

show vlan classifier rule

Overview Use this command to display information about all configured VLAN classifier rules or a specific rule.

Syntax

```
show vlan classifier rule [<1-256>]
```

Parameter	Description
<1-256>	VLAN classifier rule identifier

Mode User Exec and Privileged Exec

Usage If a rule ID is not specified, all configured VLAN classifier rules are shown. If a rule ID is specified, a specific configured VLAN classifier rule is shown.

Example To display information about VLAN classifier rule 1, enter the command:

```
awplus# show vlan classifier rule 1
```

Output Figure 13-7: Example output from the **show vlan classifier rule**1 command

```
vlan classifier group 1 add rule 1
```

Related Commands

vlan classifier activate

vlan classifier rule ipv4

vlan classifier rule proto

show vlan private-vlan

Overview Use this command to display the private VLAN configuration and associations.

Syntax

```
show vlan private-vlan
```

Mode User Exec and Privileged Exec

Example To display the private VLAN configuration and associations, enter the command:

```
awplus# show vlan private-vlan
```

Output Figure 13-8: Example output from the **show vlan private-vlan** command

```
awplus#show vlan private-vlan
 PRIMARY       SECONDARY          TYPE         INTERFACES
 -------       ---------        ----------     ----------
       2               3          isolated
       2               4         community
                       8          isolated
```

Related Commands

private-vlan

private-vlan association

show vlan statistics

Overview Use this command to display the current configuration for either a specific VLAN statistics instance, or (by not specifying an instance) display all VLAN packet counter instances.

Syntax

```
show vlan statistics [name <instance_name>]
```

Mode User Exec and Privileged Exec

Examples To display all packet counters for the packet counter instance **vlan2-data**

```
awplus# show vlan statistics name vlan2-data
```

To display all packet counters for all packet counter instances.

```
awplus# show vlan statistics
```

Table 13-2: Example output from the **show vlan statistics** command

```
VLAN Stats Collection: vlan2-data
  VLAN ID: 2
  Port Map: port1.0.1, port1.0.2, port1.0.4
  Ingress Packets: total 941, bytes 66185
```

Related Commands

clear vlan statistics

vlan statistics

switchport access vlan

Overview Use this command to change the port-based VLAN of the current port.

Use the **no** variant of this command to change the port-based VLAN of this port to the default VLAN, vlan1.

Syntax

```
switchport access vlan <vlan-id>
no switchport access vlan
```

Parameter	Description
<vlan-id>	<1-4094> The port-based VLAN ID for the port.

Default Reset the default VLAN 1 to specified switchports using the negated form of this command.

Mode Interface Configuration

Usage Any untagged frame received on this port will be associated with the specified VLAN.

Examples To change the port-based VLAN to VLAN 3 for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 3
```

To reset the port-based VLAN to the default VLAN 1 for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport access vlan
```

Validation Command show interface switchport

Related Commands show vlan

switchport enable vlan

Overview This command enables the VLAN on the port manually once disabled by certain actions, such as QSP (QoS Storm Protection) or EPSR (Ethernet Protection Switching Ring). Note that if the VID is not given, all disabled VLANs are re-enabled.

Syntax

```
switchport
enable vlan [<1-4094>]
```

Parameter	Description
`vlan`	Re-enables the VLAN on the port.
<1-4094>	VLAN ID.

Mode Interface Configuration

Example To re-enable the `port1.0.1` from VLAN 1:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport enable vlan 1
```

Related Commands show mls qos interface storm-status

storm-window

switchport mode access

Overview Use this command to set the switching characteristics of the port to access mode. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Syntax

```
switchport mode access [ingress-filter {enable|disable}]
```

Parameter	Description
`ingress-filter`	Set the ingress filtering for the received frames.
`enable`	Turn on ingress filtering for received frames. This is the default.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default By default, ports are in access mode with ingress filtering on.

Usage Use access mode to send untagged frames only.

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access ingress-filter enable
```

Validation Command show interface switchport

switchport mode private-vlan

Overview Use this command to make a Layer 2 port a private VLAN host port or a promiscuous port.

Use the **no** variant of this command to remove the configuration.

Syntax

```
switchport mode private-vlan {host|promiscuous}
no switchport mode private-vlan {host|promiscuous}
```

Parameter	Description
`host`	This port type can communicate with all other host ports assigned to the same community VLAN, but it cannot communicate with the ports in the same isolated VLAN. All communications outside of this VLAN must pass through a promiscuous port in the associated primary VLAN.
`promiscuous`	A promiscuous port can communicate with all interfaces, including the community and isolated ports within a private VLAN.

Mode Interface Configuration

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode private-vlan host
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode private-vlan promiscuous
awplus(config)# interface port1.0.4
awplus(config-if)# no switchport mode private-vlan promiscuous
```

Related Commands switchport private-vlan mapping

switchport mode private-vlan trunk promiscuous

Overview Use this command to enable a port in trunk mode to be promiscuous port for isolated VLANs.

NOTE: *Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.*

Use the **no** variant of this command to remove a port in trunk mode as a promiscuous port for isolated VLANs. You must first remove the secondary port, or ports, in trunk mode associated with the promiscuous port with the **no switchport mode private-vlan trunk secondary** command.

Syntax

```
switchport mode private-vlan trunk promiscuous group <group-id>
no switchport mode private-vlan trunk promiscuous
```

Parameter	Description
<group-id>	The group ID is a numeric value in the range 1 to 32 that is used to associate the promiscuous port with secondary ports.

Default By default, a port in trunk mode is disabled as a promiscuous port.

Mode Interface Configuration

Usage A port must be put in trunk mode with switchport mode trunk command before it can be enabled as a promiscuous port.

To add VLANs to be trunked over the promiscuous port, use the switchport trunk allowed vlan command. These VLANs can be isolated VLANs, or non-private VLANs.

To configure the native VLAN for the promiscuous port, use the switchport trunk native vlan command. The native VLAN can be an isolated VLAN, or a non-private VLAN.

When you enable a promiscuous port, all of the secondary port VLANs associated with the promiscuous port via the group ID number must be added to the promiscuous port. In other words, the set of VLANs on the promiscuous port must be a superset of all the VLANs on the secondary ports within the group.

Examples To create the isolated VLANs 2, 3 and 4 and then enable `port1.0.2` in trunk mode as a promiscuous port for these VLANs with the group ID of 3, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2-4
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# private-vlan 3 isolated
awplus(config-vlan)# private-vlan 4 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2-4
awplus(config-if)# switchport mode private-vlan trunk
promiscuous group 3
```

To remove port1.0.2 in trunk mode as a promiscuous port for a private VLAN, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport mode private-vlan trunk
promiscuous
```

Note that you must remove the secondary port or ports enabled as trunk ports that are associated with the promiscuous port before removing the promiscuous port.

Related Commands

switchport mode private-vlan trunk secondary

switchport mode trunk

switchport trunk allowed vlan

switchport trunk native vlan

show vlan private-vlan

switchport mode private-vlan trunk secondary

Overview Use this command to enable a port in trunk mode to be a secondary port for isolated VLANs.

NOTE: *Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. Private VLAN trunk ports and GVRP are mutually exclusive.*

Use the **no** variant of this command to remove a port in trunk mode as a secondary port for isolated VLANs.

Syntax

```
switchport mode private-vlan trunk secondary group <group-id>
no switchport mode private-vlan trunk secondary
```

Parameter	Description
<group-id>	The group ID is a numeric value in the range 1 to 32 that is used to associate a secondary port with its promiscuous port.

Default By default, a port in trunk mode is disabled as a secondary port.

When a port in trunk mode is enabled to be a secondary port for isolated VLANs, by default it will have a native VLAN of **none**(no native VLAN specified).

Mode Interface Configuration

Usage A port must be put in trunk mode with switchport mode trunk command before the port is enabled as a secondary port in trunk mode.

To add VLANs to be trunked over the secondary port use the switchport trunk allowed vlan command. These must be isolated VLANs and must exist on the associated promiscuous port.

To configure the native VLAN for the secondary port, use the switchport trunk native vlan command. The native VLAN must be an isolated VLAN and must exist on the associated promiscuous port.

Examples

To create isolated private VLAN 2 and then enable `port1.0.3` in trunk mode as a secondary port for the this VLAN with the group ID of `3`, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 2
awplus(config-vlan)# private-vlan 2 isolated
awplus(config-vlan)# exit
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk
awplus(config-if)# switchport trunk allowed vlan add 2
awplus(config-if)# switchport mode private-vlan trunk secondary
group 3
```

To remove port1.0.3 in trunk mode as a secondary port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no switchport mode private-vlan trunk
secondary
```

Related Commands

switchport mode private-vlan trunk promiscuous

switchport mode trunk

switchport trunk allowed vlan

switchport trunk native vlan

show vlan private-vlan

switchport mode trunk

Overview Use this command to set the switching characteristics of the port to trunk. Received frames are classified based on the VLAN characteristics, then accepted or discarded based on the specified filtering criteria.

Syntax

```
switchport mode trunk [ingress-filter {enable|disable}]
```

Parameter	Description
`ingress-filter`	Set the ingress filtering for the frames received.
`enable`	Turn on ingress filtering for received frames. This is the default.
`disable`	Turn off ingress filtering to accept frames that do not meet the classification criteria.

Default By default, ports are in access mode, are untagged members of the default VLAN (vlan1), and have ingress filtering on.

Mode Interface Configuration

Usage A port in trunk mode can be a tagged member of multiple VLANs, and an untagged member of one native VLAN.

To configure which VLANs this port will trunk for, use the switchport trunk allowed vlan command.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# switchport mode trunk ingress-filter enable
```

Validation Command show interface switchport

switchport private-vlan host-association

Overview Use this command to associate a primary VLAN and a secondary VLAN to a host port. Only one primary and secondary VLAN can be associated to a host port.

Use the **no** variant of this command to remove the association.

Syntax

```
switchport private-vlan host-association <primary-vlan-id> add
<secondary-vlan-id>
no switchport private-vlan host-association
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vlan-id>	VLAN ID of the secondary VLAN (either isolated or community).

Mode Interface Configuration

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan host-association 2
add 3
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport private-vlan host-association
```

switchport private-vlan mapping

Overview Use this command to associate a primary VLAN and a set of secondary VLANs to a promiscuous port.

Use the **no** variant of this to remove all the association of secondary VLANs to primary VLANs for a promiscuous port.

Syntax

```
switchport private-vlan mapping <primary-vlan-id> add
<secondary-vid-list>
```

```
switchport private-vlan mapping <primary-vlan-id> remove
<secondary-vid-list>
```

```
no switchport private-vlan mapping
```

Parameter	Description
<primary-vlan-id>	VLAN ID of the primary VLAN.
<secondary-vid-list>	VLAN ID of the secondary VLAN (either isolated or community), or a range of VLANs, or a comma-separated list of VLANs and ranges.

Mode Interface Configuration

Usage This command can be applied to a switch port or a static channel group, but not a dynamic (LACP) channel group. LACP channel groups (dynamic/LACP aggregators) cannot be promiscuous ports in private VLANs.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport private-vlan mapping 2 add 3-4
awplus(config-if)# switchport private-vlan mapping 2 remove 3-4
awplus(config-if)# no switchport private-vlan mapping
```

Related Commands switchport mode private-vlan

switchport trunk allowed vlan

Overview Use this command to add VLANs to be trunked over this switch port. Traffic for these VLANs can be sent and received on the port.

Use the **no** variant of this command to reset switching characteristics of a specified interface to negate a trunked configuration specified with **switchport trunk allowed vlan** command.

Syntax

```
switchport trunk allowed vlan all
switchport trunk allowed vlan none
switchport trunk allowed vlan add <vid-list>
switchport trunk allowed vlan remove <vid-list>
switchport trunk allowed vlan except <vid-list>
no switchport trunk
```

Parameter	Description
`all`	Allow all VLANs to transmit and receive through the port.
`none`	Allow no VLANs to transmit and receive through the port.
`add`	Add a VLAN to transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.
`remove`	Remove a VLAN from transmit and receive through the port. Only use this parameter if a list of VLANs are already configured on a port.
`except`	All VLANs, except the VLAN for which the VID is specified, are part of its port member set. Only use this parameter to remove VLANs after either this parameter or the **all** parameter have added VLANs to a port.
<vid-list>	<2-4094> The ID of the VLAN or VLANs that will be added to, or removed from, the port. A single VLAN, VLAN range, or comma-separated VLAN list can be set. For a VLAN range, specify two VLAN numbers: lowest, then highest number in the range, separated by a hyphen. For a VLAN list, specify the VLAN numbers separated by commas. Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

Default By default, ports are untagged members of the default VLAN (vlan1).

Mode Interface Configuration

Usage The **all** parameter sets the port to be a tagged member of all the VLANs configured on the device. The **none** parameter removes all VLANs from the port's tagged member set. The **add** and **remove** parameters will add and remove VLANs to and from the port's member set. See the note below about restrictions when using the **add**, **remove**, **except**, and **all** parameters.

NOTE: *Only use the **add** or the **remove** parameters with this command if a list of VLANs are configured on a port. Only use the **except** parameter to remove VLANs after either the **except** or the **all** parameters have first been used to add a list of VLANs to a port.*

To remove a VLAN, where the configuration for `port1.0.6` shows the below output:

```
awplus#show running-config

!
interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 4
```

Remove VLAN `3` by re-entering the **except** parameter with the list of VLANs to remove, instead of using the **remove** parameter, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# switchport trunk allowed vlan except 3,4
```

Then the configuration is changed after entering the above commands to remove VLAN 3:

```
awplus#show running-config

!

interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-4
```

To add a VLAN, where the configuration for `port1.0.6` shows the below output:

```
awplus#show running-config

!

interface port1.0.6
switchport
switchport mode trunk
switchport trunk allowed vlan except 3-5
```

Add VLAN 4 by re-entering the **except** parameter with a list of VLANs to exclude, instead of using the **add** parameter to include VLAN 4, as shown in the command example below:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport trunk allowed vlan except 3,5
```

The configuration is changed after entering the above commands to add VLAN 4:

```
awplus#show running-config

!

interface port1.0.5
switchport
switchport mode trunk
switchport trunk allowed vlan except 3,5
```

Examples The following shows adding a single VLAN to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2
```

The following shows adding a range of VLANs to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2-4
```

The following shows adding a list of VLANs to the port's member set.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk allowed vlan add 2,3,4
```

switchport trunk native vlan

Overview Use this command to configure the native VLAN for this port. The native VLAN is used for classifying the incoming untagged packets. Use the **none** parameter with this command to remove the native VLAN from the port and set the acceptable frame types to vlan-tagged only.

Use the **no** variant of this command to revert the native VLAN to the default VLAN ID 1. Command negation removes tagged VLANs, and sets the native VLAN to the default VLAN.

Syntax

```
switchport trunk native vlan {<vid>|none}
no switchport trunk native vlan
```

Parameter	Description
`<vid>`	`<2-4094>` The ID of the VLAN that will be used to classify the incoming untagged packets. The VLAN ID must be a part of the VLAN member set of the port.
`none`	No native VLAN specified. This option removes the native VLAN from the port and sets the acceptable frame types to vlan-tagged only. Note: Use the **no** variant of this command to revert to the default VLAN 1 as the native VLAN for the specified interface switchport - not **none**.

Default VLAN 1 (the default VLAN), which is reverted to using the **no** form of this command.

Mode Interface Configuration

Examples The following commands show configuration of VLAN 2 as the native VLAN for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan 2
```

The following commands show the removal of the native VLAN for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport trunk native vlan none
```

The following commands revert the native VLAN to the default VLAN 1 for interface `port1.0.2`:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no switchport trunk native vlan
```

switchport vlan translation

Overview Use this command to create a VLAN translation entry on an interface. The translation entry translates a packet's VLAN-ID as seen on the wire.

Use the **no** variant of this command to remove all translation entries or a specific entry.

This command can be applied to a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Syntax

```
switchport vlan translation vlan <wire-vid> vlan <vid>
no switchport vlan translation [all|vlan <wire-vid>]
```

Parameter	Description
`vlan <wire-vid>`	VLAN-ID of the packet as you want it to be seen on the wire.
`vlan <vid>`	VLAN-ID of the VLAN as it was assignedwhen the VLAN was created.
`all`	Delete all translation entries.

Default None (by default, no translation entries exist)

Mode Interface Configuration for a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Example To translate VLAN100 to VLAN200 on port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation vlan 200 vlan 100
```

Related Commands

show interface switchport vlan translation

switchport vlan translation default drop

switchport vlan translation default drop

Overview Use this command to configure a default behavior of dropping inbound tagged packets that have a VLAN-ID that does not match any entries in the VLAN translation table for an interface.

Use the **no** variant of this command to stop dropping non-matching inbound packets and let them be accepted as is for further processing.

Syntax

```
switchport vlan translation default drop
no switchport vlan translation default drop
```

Default Do not drop packets

Mode Interface Configuration for a switch port or a static channel group, or a dynamic (LACP) channel group. The interface must be in a mode that supports tagged packets.

Example To drop inbound tagged packets arriving at port1.0.1 unless they match a VLAN translation entry, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport vlan translation default drop
```

To accept inbound tagged packets arriving at port1.0.1 regardless of whether they match a VLAN translation entry, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no switchport vlan translation default drop
```

Related Commands

show interface switchport vlan translation

switchport vlan translation default drop

switchport vlan-stacking (double tagging)

Overview Use this command to enable VLAN stacking on a port and set it to be a customer-edge-port or provider-port. This is sometimes referred to as VLAN double-tagging, nested VLANs, or Q in Q.

Use **no** parameter with this command to disable VLAN stacking on an interface.

Syntax

```
switchport vlan-stacking {customer-edge-port|provider-port}
no switchport vlan-stacking
```

Parameter	Description
`customer-edge-port`	Set the port to be a customer edge port. This port must already be in access mode.
`provider-port`	Set the port to be a provider port. This port must already be in trunk mode.

Default By default, ports are not VLAN stacking ports.

Mode Interface Configuration

Usage Use VLAN stacking to separate traffic from different customers to that they can be managed over a provider network.

Note that you must also set an MRU of 1504 or higher on the customer edge port, using the mru command.

Traffic with an extra VLAN header added by VLAN stacking cannot be routed.

Example To apply vlan-stacking to the selected port, configure it to be a customer edge port, and increase the MRU, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport vlan-stacking customer-edge-port
awplus(config-if)# mru 10240
```

switchport voice dscp

Overview Use this command for a specific port to configure the Layer 3 DSCP value advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified DSCP value.

Use the **no** variant of this command to reset the DSCP value to the default, 0.

Syntax

```
switchport voice dscp <0-63>
no switchport voice dscp
```

Parameter	Description
`dscp`	Specify a DSCP value for voice data.
<0-63>	DSCP value.

Default A DSCP value of 0 will be advertised.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port (switchport voice vlan command)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port

Example To tell IP phones connected to `port1.0.5` to send voice data with DSCP value 27, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice dscp 27
```

Related Commands

lldp med-tlv-select

show lldp

switchport voice vlan

switchport voice vlan

Overview Use this command to configure the Voice VLAN tagging advertised when the transmission of LLDP-MED Network Policy TLVs for voice endpoint devices is enabled. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified tagging. This command also sets the ports to be spanning tree edge ports, that is, it enables spanning tree portfast on the ports.

Use the **no** variant of this command to remove LLDP-MED network policy configuration for voice devices connected to these ports. This does not change the spanning tree edge port status.

Syntax

```
switchport voice vlan [<vid>|dot1p|dynamic|untagged]
no switchport voice vlan
```

Parameter	Description
`<vid>`	VLAN identifier, in the range 1 to 4094.
`dot1p`	The IP phone should send User Priority tagged packets, that is, packets in which the tag contains a User Priority value, and a VID of 0. (The User Priority tag is also known as the 802.1p priority tag, or the Class of Service (CoS) tag.)
`dynamic`	The VLAN ID with which the IP phone should send tagged packets will be assigned by RADIUS authentication.
`untagged`	The IP phone should send untagged packets.

Default By default, no Voice VLAN is configured, and therefore no network policy is advertised for voice devices.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port using this command (switchport voice vlan)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port.

To set the priority value to be advertised for tagged frames, use the switchport voice vlan priority command.

If the Voice VLAN details are to be assigned by RADIUS, then the RADIUS server must be configured to send the attribute "Egress-VLANID (56)" or "Egress-VLAN-Name (58)" in the RADIUS Accept message when authenticating a phone attached to this port.

To set these attributes on the local RADIUS server, use the egress-vlan-id command or the egress-vlan-name command.

For more information about configuring authentication for Voice VLAN, see the LLDP Feature Overview and Configuration Guide.

If the ports have been set to be edge ports by the switchport voice vlan command, the **no** variant of this command will leave them unchanged as edge ports. To set them back to their default non-edge port configuration, use the spanning-tree edgeport (RSTP and MSTP) command.

Examples To tell IP phones connected to `port1.0.5` to send voice data tagged for VLAN 10, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# switchport voice vlan 10
```

To tell IP phones connected to ports 1.0.2-1.0.6 to send priority tagged packets (802.1p priority tagged with VID 0, so that they will be assigned to the port VLAN) use the following commands. The priority value is 5 by default, but can be configured with the switchport voice vlan priority command.

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.6
awplus(config-if)# switchport voice vlan dot1p
```

To dynamically configure the VLAN ID advertised to IP phones connected to `port1.0.1` based on the VLAN assigned by RADIUS authentication (with RADIUS attribute "Egress- VLANID" or "Egress-VLAN-Name" in the RADIUS accept packet), use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport voice vlan dynamic
```

To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on `port1.0.6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

Related Commands

egress-vlan-id

egress-vlan-name

lldp med-tlv-select

spanning-tree edgeport (RSTP and MSTP)

switchport voice dscp

switchport voice vlan priority

show lldp

switchport voice vlan priority

Overview Use this command to configure the Layer 2 user priority advertised when the transmission of LLDP-MED Network Policy TLVs for voice devices is enabled. This is the priority in the User Priority field of the IEEE 802.1Q VLAN tag, also known as the Class of Service (CoS), or 802.1p priority. When LLDP-MED capable IP phones receive this network policy information, they transmit voice data with the specified priority.

Syntax

```
switchport voice vlan priority <0-7>
no switchport voice vlan priority
```

Parameter	Description
`priority`	Specify a user priority value for voice data.
<0-7>	Priority value.

Default By default, the Voice VLAN user priority value is 5.

Mode Interface Configuration

Usage LLDP-MED advertisements including Network Policy TLVs are transmitted via a port if:

- LLDP is enabled (lldp run command)
- Voice VLAN is configured for the port (switchport voice vlan command)
- The port is configured to transmit LLDP advertisements—enabled by default (lldp transmit receive command)
- The port is configured to transmit Network Policy TLVs—enabled by default (lldp med-tlv-select command)
- There is an LLDP-MED device connected to the port.

To set the Voice VLAN tagging to be advertised, use the switchport voice vlan command.

Example To remove the Voice VLAN, and therefore disable the transmission of LLDP-MED network policy information for voice devices on `port1.0.6`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no switchport voice vlan
```

Related Commands

lldp med-tlv-select

show lldp

switchport voice vlan

vlan

Overview This command creates VLANs, assigns names to them, and enables or disables them. Specifying the `disable` state causes all forwarding over the specified VLAN ID to cease. Specifying the `enable` state allows forwarding of frames on the specified VLAN.

The **no** variant of this command destroys the specified VLANs.

Syntax

```
vlan <vid> [name <vlan-name>] [state {enable|disable}]
vlan <vid-range> [state {enable|disable}]
vlan {<vid>|<vlan-name>} [mtu <mtu-value>]
no vlan {<vid>|<vid-range>} [mtu]
```

Parameter	Description
<vid>	The VID of the VLAN to enable or disable in the range < **1-4094**>.
<vlan-name>	The ASCII name of the VLAN. Maximum length: **32** characters.
<vid-range>	Specifies a range of VLAN identifiers.
<mtu-value>	Specifies the Maximum Transmission Unit (MTU) size in bytes, in the range 68 to1500 bytes, for the VLAN.
`enable`	Sets VLAN into an `enable` state.
`disable`	Sets VLAN into a `disable` state.

Default By default, VLANs are enabled when they are created.

Mode VLAN Configuration

Examples

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 45 name accounts state enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 45
```

Related Commands mtu

vlan database

show vlan

vlan classifier activate

Overview Use this command in Interface Configuration mode to associate a VLAN classifier group with the switch port.

Use the **no** variant of this command to remove the VLAN classifier group from the switch port.

Syntax

```
vlan classifier activate <vlan-class-group-id>
no vlan classifier activate <vlan-class-group-id>
```

Parameter	Description
<vlan-class-group-id>	Specify a VLAN classifier group identifier in the range <1-16>.

Mode Interface Configuration mode for a switch port.

Usage See the protocol-based VLAN configuration example in the VLAN Feature Overview and Configuration Guide for configuration details.

You cannot enter this command on a link aggregator. Enter it on the aggregator's switch ports instead.

Example To associate VLAN classifier group 3 with switch `port1.0.3`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# vlan classifier activate 3
```

To remove VLAN classifier group 3 from switch `port1.0.3`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no vlan classifier activate 3
```

Related Commands

show vlan classifier rule

vlan classifier group

vlan classifier rule ipv4

vlan classifier rule proto

vlan classifier group

Overview Use this command to create a group of VLAN classifier rules. The rules must already have been created.

Use the **no** variant of this command to delete a group of VLAN classifier rules.

Syntax

```
vlan classifier group <1-16> {add|delete} rule
<vlan-class-rule-id>
```

```
no vlan classifier group <1-16>
```

Parameter	Description
<1-16>	VLAN classifier group identifier
add	Add the rule to the group.
delete	Delete the rule from the group.
<vlan-class-rule-id>	The VLAN classifier rule identifier.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# vlan classifier group 3 add rule 5
```

Related Commands

show vlan classifier rule

vlan classifier activate

vlan classifier rule ipv4

vlan classifier rule proto

vlan classifier rule ipv4

Overview Use this command to create an IPv4 subnet-based VLAN classifier rule and map it to a specific VLAN. Use the **no** variant of this command to delete the VLAN classifier rule.

Syntax

```
vlan classifier rule <1-256> ipv4 <ip-addr/prefix-length> vlan <1-4094>
no vlan classifier rule <1-256>
```

Parameter	Description
<1-256>	Specify the VLAN Classifier Rule identifier.
<ip-addr/prefix-length>	Specify the IP address and prefix length.
<1-4094>	Specify a VLAN ID to which an untagged packet is mapped in the range *<1-4094>*.

Mode Global Configuration

Usage If the source IP address matches the IP subnet specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN.

Example

```
awplus# configure terminal
awplus(config)# vlan classifier rule 3 ipv4 3.3.3.3/8 vlan 5
```

Related Commands

show vlan classifier rule

vlan classifier activate

vlan classifier rule proto

vlan classifier rule proto

Overview Use this command to create a protocol type-based VLAN classifier rule, and map it to a specific VLAN. See the published IANA EtherType IEEE 802 numbers here:

www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt.

Instead of a protocol name the decimal value of the protocol's EtherType can be entered. The EtherType field is a two-octet field in an Ethernet frame. It is used to show which protocol is encapsulated in the payload of the Ethernet frame. Note that EtherTypes in the IANA 802 numbers are given as hexadecimal values.

The **no** variant of this command removes a previously set rule.

Syntax

```
vlan classifier rule <1-256> proto <protocol> encap
{ethv2|nosnapllc|snapllc} vlan <1-4094>
```

```
no vlan classifier rule <1-256>
```

Parameter	Description	
<1-256>	VLAN Classifier identifier	
proto	Protocol type	
<protocol>	Specify a protocol either by its decimal number (0-65535) or by one of the following protocol names:	
	[arp|2054]	Address Resolution protocol
	[atalkaarp|33011]	Appletalk AARP protocol
	[atalkddp|32923]	Appletalk DDP protocol
	[atmmulti|34892]	MultiProtocol Over ATM protocol
	[atmtransport|34948]	Frame-based ATM Transport protocol
	[dec|24576]	DEC Assigned protocol
	[deccustom|24582]	DEC Customer use protocol
	[decdiagnostics|24581]	DEC Systems Comms Arch protocol
	[decdnadumpload|24577]	DEC DNA Dump/Load protocol
	[decdnaremoteconsole|24578]	DEC DNA Remote Console protocol
	[decdnarouting|24579]	DEC DNA Routing protocol
	[declat|24580]	DEC LAT protocol

Parameter	Description	
	`[decsyscomm|24583]`	DEC Systems Comms Arch protocol
	`[g8bpqx25|2303]`	G8BPQ AX.25 protocol
	`[ieeeaddrtrans|2561]`	Xerox IEEE802.3 PUP Address
	`[ieeepup|2560]`	Xerox IEEE802.3 PUP protocol
	`[ip|2048]`	IP protocol
	`[ipv6|34525]`	IPv6 protocol
	`[ipx|33079]`	IPX protocol
	`[netbeui|61680]`	IBM NETBIOS/NETBEUI protocol
	`[netbeui|61681]`	IBM NETBIOS/NETBEUI protocol
	`[pppdiscovery|34915]`	PPPoE discovery protocol
	`[pppsession|34916]`	PPPoE session protocol
	`[rarp|32821]`	Reverse Address Resolution protocol
	`[x25|2056]`	CCITT.25 protocol
	`[xeroxaddrtrans|513]`	Xerox PUP Address Translation protocol
	`[xeroxpup|512]`	Xerox PUP protocol
`ethv2`	Ethernet Version 2 encapsulation	
`nosnapllc`	LLC without SNAP encapsulation	
`snapllc`	LLC SNAP encapsulation	
<1-4094>	Specify a VLAN ID to which an untagged packet is mapped in the range *<1-4094>*	

Mode Global Configuration

Usage If the protocol type matches the protocol specified in the VLAN classifier rule, the received packets are mapped to the specified VLAN. Ethernet Frame Numbers may be entered in place of the protocol names listed. For a full list please refer to the IANA list online:www.iana.org/assignments/ieee-802-numbers/ieee-802-numbers.txt

Examples

```
awplus# configure terminal
awplus(config)# vlan classifier rule 1 proto x25 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 2 proto 512 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 3 proto 2056 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 4 proto 2054 encap ethv2 vlan 2
awplus(config)# vlan classifier rule 5 proto  encap ethv2 vlan 234525
awplus(config)# vlan classifier rule 6 proto  encap ethv2 vlan 2ipv6
awplus(config)# vlan classifier rule 7 proto  encap ethv2 vlan 22048
awplus(config)# vlan classifier rule 8 proto  encap ethv2 vlan 2ip
```

Validation Output

```
awplus# show vlan classifier rule
```

```
vlan classifier rule 16 proto rarp encap ethv2 vlan 2

vlan classifier rule 8 proto encap ethv2 vlan 2

vlan classifier rule 4 proto arp encap ethv2 vlan 2

vlan classifier rule 3 proto xeroxpup encap ethv2 vlan 2
vlan classifier rule 2 proto ip encap ethv2 vlan 2
vlan classifier rule 1 proto ipv6 encap ethv2 vlan 2
```

Related Commands

show vlan classifier rule

vlan classifier activate

vlan classifier group

vlan database

Overview Use this command to enter the VLAN Configuration mode.

Syntax

```
vlan database
```

Mode Global Configuration

Usage Use this command to enter the VLAN configuration mode. You can then add or delete a VLAN, or modify its values.

Example In the following example, note the change to VLAN configuration mode from Configure mode:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)#
```

Related Commands vlan

vlan mode stack-local-vlan

Overview This command enables you to create stack-local-VLANs and use ICMP to monitor and diagnose issues within specific members of the stack. When a VLAN is added using this method, all its traffic will be trapped to and processed by the CPU of the specific local stack member, rather than the CPU of the stack master.

Syntax

```
vlan <vid> mode stack-local-vlan <member-id>
no vlan <vid>
```

Parameter	Description
<vid>	The VID of the VLAN to be created in the range 2-4094. We recommend that the first stack-local-vlan be assigned the number 4001 for the first stack member, then incremented by one for each stack member. For example, a stack of four members would be assigned the following VID numbers: • stack member one: VID 4001 • stack member two: VID 4002 • stack member three: VID 4003 • stack member four: VID 4004
`mode stack-local-vlan`	Specifies that the new VLAN will function as a stack-local-VLAN.
<member-id>	Specifies the new stack member ID. Enter a decimal number in the range 1-8.

Default By default, VLANs are automatically enabled as they are added.

Mode VLAN Configuration

Usage If IGMP snooping is operating on a stack-local-VLAN, the device will try to process some multicast traffic via that VLAN, if it is connected to a Microsoft Windows PC.

To avoid this, we recommend disabling IGMP snooping on stack-local-VLANs, by using the command **no** ip igmp snooping.

Examples To add a stack-local-VLAN with the VID of 4002 and assign it to stack member 2, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 4002 mode stack-local-vlan 2
awplus(config-vlan)# exit
awplus(config)# interface vlan4002
awplus(config-if)# no ip igmp snooping
```

To remove VLAN 4002, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 4002
```

Related Commands

ip igmp snooping

mtu

vlan database

vlan statistics

Overview This command creates a VLAN packet counter instance, and enables you to add one or more ports to a defined counter instance. This command can only be applied to switch ports. You cannot apply it to aggregated links or eth ports.

The **no** variant of this command enables the deletion of VLAN packet counter instances, or for removing one or more ports that are currently mapped to a counter instance. Note that the selected range of ports must all be switch ports.

NOTE:

In describing this command, the terms frame and packet are used interchangeably.

Syntax

```
vlan <vid> statistics name <instance_name>
no vlan statistics name <instance_name>
```

Parameter	Description
<vid>	The VID of the VLAN that is associated with *<instance-name>*.
<instance-name>	The name of the instance for which incoming frames and their bytes are counted.

Mode Interface Configuration

Usage A maximum of 128 packet counter instances can be created. When the first instance is configured, the switch will reserve sufficient resources to support 128 packet counter instances. These resources are also shared with other features such as QoS and ACLs. Where the remaining resources are insufficient to support the VLAN Statistics feature the feature will not be enabled, and an error message will display.

Examples Create a VLAN packet counter instance named **vlan2-data**, and apply this to count incoming vlan2 tagged frames on ports 1.0.4 and 1.0.5.

```
awplus# configure terminal
awplus(config)# interface port1.0.4,port1.0.5
awplus(config-if)# vlan 2 statistics name vlan2-data
```

From the previous example, add ports in the range 1.0.2 to 1.0.3 to the VLAN packet counter instance. The **vlan2-data** instance will now count all incoming vlan2 tagged frames on ports within the range 1.0.1 to 1.0.5.

```
awplus(config)# interface port1.0.2-port1.0.3
awplus(config-if)# vlan 2 statistics name vlan2-data
```

To remove `port1.0.5` from the packet counter instance named **vlan2-data.**

```
awplus(config)# interface port1.0.5
awplus(config-if)# no vlan statistics name vlan2-data
```

To remove the remaining ports 1.0.2 to 1.0.4 from the packet counter instance named **vlan2-data.** Note that because there are no ports associated with the **vlan2-data**, this instance will be removed.

```
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# no vlan statistics name vlan2-data
```

Related Commands

clear vlan statistics

show vlan statistics

14 Spanning Tree Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure RSTP, STP or MSTP. For information about spanning trees, including configuration procedures, see the STP Feature Overview and Configuration Guide.

Command List

clear spanning-tree statistics

Overview Use this command to clear all the STP BPDU (Bridge Protocol Data Unit) statistics.

Syntax

```
clear spanning-tree statistics
clear spanning-tree statistics [instance <mstp-instance>]
clear spanning-tree statistics [interface <port> [instance
<mstp-instance>]]
```

Parameter	Description
<port>	The port to clear STP BPDU statistics for. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).
<mstp-instance>	The MSTP instance (MSTI - Multiple Spanning Tree Instance) to clear MSTP BPDU statistics.

Mode User Exec and Privileged Exec

Usage Use this command with the **instance** parameter in MSTP mode. Specifying this command with the **interface** parameter only not the instance parameter will work in STP and RSTP mode.

Examples

```
awplus# clear spanning-tree statistics
awplus# clear spanning-tree statistics instance 1
awplus# clear spanning-tree statistics interface port1.0.2
awplus# clear spanning-tree statistics interface port1.0.2
instance 1
```

clear spanning-tree detected protocols (RSTP and MSTP)

Overview Use this command to clear the detected protocols for a specific port, or all ports.

Use this command in RSTP or MSTP mode only.

Syntax

```
clear spanning-tree detected protocols [interface <port>]
```

Parameter	Description
<port>	The port to clear detected protocols for. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example

```
awplus# clear spanning-tree detected protocols
```

debug mstp (RSTP and STP)

Overview Use this command to enable debugging for the configured spanning tree mode, and echo data to the console, at various levels. Note that although this command uses the keyword **mstp** it displays debugging output for RSTP and STP protocols as well the MSTP protocol.

Use the **no** variant of this command to disable spanning tree debugging.

Syntax

```
debug mstp {all|cli|protocol [detail]|timer [detail]}
debug mstp {packet {rx|tx} [decode] [interface <interface>]}
debug mstp {topology-change [interface <interface>]}
no debug mstp {all|cli|protocol [detail]|timer [detail]}
no debug mstp {packet {rx|tx} [decode] [interface <interface>]}
no debug mstp {topology-change [interface <interface>]}
```

Parameter	Description
`all`	Echoes all spanning tree debugging levels to the console.
`cli`	Echoes spanning tree commands to the console.
`packet`	Echoes spanning tree packets to the console.
`rx`	Received packets.
`tx`	Transmitted packets.
`protocol`	Echoes protocol changes to the console.
`timer`	Echoes timer information to the console.
`detail`	Detailed output.
`decode`	Interprets packet contents
`topology-change`	Interprets topology change messages
`interface`	Keyword before <interface> placeholder to specify an interface to debug
<interface>	Placeholder used to specify the name of the interface to debug.

Mode Privileged Exec and Global Configuration mode

Usage 1 Use the **debug mstp topology-change interface** command to generate debugging messages when the device receives an indication of a topology change in a BPDU from another device. The debugging can be activated on a per-port basis. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the terminal monitor command before issuing the relevant **debug mstp**

command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using log buffered (filter) command:

```
awplus# configure terminal
awplus(config)# log buffered program mstp
```

Output 1

```
awplus#terminal monitor
awplus#debug mstp topology-change interface port1.0.4
10:09:09 awplus MSTP[1409]: Topology change rcvd on port1.0.4 (internal)
10:09:09 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.4
aawplus#debug mstp topology-change interface port1.0.6
10:09:29 awplus MSTP[1409]: Topology change rcvd on port1.0.6 (external)
10:09:29 awplus MSTP[1409]: Topology change rcvd on MSTI 1 port1.0.6
```

Usage 2 Use the **debug mstp packet rx|tx decode interface** command to generate debugging messages containing the entire contents of a BPDU displayed in readable text for transmitted and received xSTP BPDUs. The debugging can be activated on a per-port basis and transmit and receive debugging is controlled independently. Although this command uses the keyword **mstp**, it displays debugging output for RSTP and STP protocols as well as the MSTP protocol.

Due to the likely volume of output, these debug messages are best viewed using the terminal monitor command before issuing the relevant **debug mstp** command. The default terminal monitor filter will select and display these messages. Alternatively, the messages can be directed to any of the other log outputs by adding a filter for the MSTP application using the log buffered (filter) command:

```
awplus(config)# log buffered program mstp
```

Output 2 In MSTP mode - an MSTP BPDU with 1 MSTI:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:23:42 awplus MSTP[1417]: Protocol version: MSTP, BPDU type: RST
17:23:42 awplus MSTP[1417]: CIST Flags:  Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: CIST root id      : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST ext pathcost : 0
17:23:42 awplus MSTP[1417]: CIST reg root id  : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST port id      : 8001 (128:1)
17:23:42 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:23:42 awplus MSTP[1417]: Version 3 length : 80
17:23:42 awplus MSTP[1417]: Format id      : 0
17:23:42 awplus MSTP[1417]: Config name    : test
17:23:42 awplus MSTP[1417]: Revision level : 0
17:23:42 awplus MSTP[1417]: Config digest  : 3ab68794d602fdf43b21c0b37ac3bca8
17:23:42 awplus MSTP[1417]: CIST int pathcost : 0
17:23:42 awplus MSTP[1417]: CIST bridge id    : 0000:0000cd1000fe
17:23:42 awplus MSTP[1417]: CIST hops remaining : 20
17:23:42 awplus MSTP[1417]: MSTI flags           : Agree Forward Learn role=Desig
17:23:42 awplus MSTP[1417]: MSTI reg root id     : 8001:0000cd1000fe
17:23:42 awplus MSTP[1417]: MSTI pathcost        : 0
17:23:42 awplus MSTP[1417]: MSTI bridge priority : 32768 port priority : 128
17:23:42 awplus MSTP[1417]: MSTI hops remaining  : 20
17:23:42 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

In STP mode transmitting a TCN BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet tx decode interface port1.0.4
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - start
17:28:09 awplus MSTP[1417]: Protocol version: STP, BPDU type: TCN
17:28:09 awplus MSTP[1417]: port1.0.4 xSTP BPDU tx - finish
```

In STP mode receiving an STP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
17:31:36 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:31:36 awplus MSTP[1417]: Protocol version: STP, BPDU type: Config
17:31:36 awplus MSTP[1417]: Flags:  role=none
17:31:36 awplus MSTP[1417]: Root id      : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Root pathcost : 0
17:31:36 awplus MSTP[1417]: Bridge id  : 8000:0000cd1000fe
17:31:36 awplus MSTP[1417]: Port id      : 8001 (128:1)
17:31:36 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:31:36 awplus MSTP[1417]: ort1.0.4 xSTP BPDU rx - finish
```

In RSTP mode receiving an RSTP BPDU:

```
awplus#terminal monitor
awplus#debug mstp packet rx decode interface port1.0.4
awplus#17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - start
17:30:17 awplus MSTP[1417]: Protocol version: RSTP, BPDU type: RST
17:30:17 awplus MSTP[1417]: CIST Flags:  Forward Learn role=Desig
17:30:17 awplus MSTP[1417]: CIST root id      : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST ext pathcost : 0
17:30:17 awplus MSTP[1417]: CIST reg root id  : 8000:0000cd1000fe
17:30:17 awplus MSTP[1417]: CIST port id      : 8001 (128:1)
17:30:17 awplus MSTP[1417]: msg age: 0 max age: 20 hellotime: 2 fwd delay: 15
17:30:17 awplus MSTP[1417]: port1.0.4 xSTP BPDU rx - finish
```

Examples

```
awplus# debug mstp all
awplus# debug mstp cli
awplus# debug mstp packet rx
awplus# debug mstp protocol detail
awplus# debug mstp timer
awplus# debug mstp packet rx decode interface port1.0.2
awplus# debug mstp packet tx decode interface port1.0.6
```

Related Commands

log buffered (filter)

show debugging mstp

terminal monitor

undebug mstp

instance priority (MSTP)

Overview Use this command to set the priority for this device to become the root bridge for the specified MSTI (Multiple Spanning Tree Instance).

Use this command for MSTP only.

Use the **no** variant of this command to restore the root bridge priority of the device for the instance to the default.

Syntax

```
instance <instance-id> priority <priority>
no instance <instance-id> priority
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<priority>	Specify the root bridge priority for the device for the MSTI in the range <0-61440>. Note that a lower priority number indicates a greater likelihood of the device becoming the root bridge. The priority values can be set only in increments of 4096. If you specify a number that is not a multiple of 4096, it will be rounded down. The default priority is 32768.

Default The default priority value for all instances is 32768.

Mode MST Configuration

Usage MSTP lets you distribute traffic more efficiently across a network by blocking different links for different VLANs. You do this by making different devices into the root bridge for each MSTP instance, so that each instance blocks a different link.

If all devices have the same root bridge priority for the instance, MSTP selects the device with the lowest MAC address to be the root bridge. Give the device a higher priority for becoming the root bridge for a particular instance by assigning it a lower priority number, or vice versa.

Examples To set the root bridge priority for MSTP instance 2 to be the highest (0), so that it will be the root bridge for this instance when available, use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 priority 0
```

To reset the root bridge priority for instance 2 to the default (32768), use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# no instance 2 priority
```

Related Commands

region (MSTP)

revision (MSTP)

show spanning-tree mst config

spanning-tree mst instance

spanning-tree mst instance priority

instance vlan (MSTP)

Overview Use this command to create an MST Instance (MSTI), and associate the specified VLANs with it. An MSTI is a spanning tree instance that exists within an MST region (MSTR).

When a VLAN is associated with an MSTI the member ports of the VLAN are automatically configured to send and receive spanning-tree information for the associated MSTI. You can disable this automatic configuration of member ports of the VLAN to the associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI.

Use the **instance vlan** command for MSTP only.

Use the **no** variant of this command to remove the specified VLANs from the MSTI.

Syntax

```
instance <instance-id> vlan <vid-list>
no instance <instance-id> vlan <vid-list>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<vid-list>	Specify one or more VLAN identifiers (VID) to be associated with the MSTI specified. This can be a single VID in the range 1-4094, or a hyphen-separated range or a comma-separated list of VLAN IDs.

Mode MST Configuration

Usage The VLANs must be created before being associated with an MST instance (MSTI). If the VLAN range is not specified, the MSTI will not be created.

This command removes the specified VLANs from the CIST and adds them to the specified MSTI. If you use the **no** variant of this command to remove the VLAN from the MSTI, it returns it to the CIST. To move a VLAN from one MSTI to another, you must first use the **no** variant of this command to return it to the CIST.

Ports in these VLANs will remain in the control of the CIST until you associate the ports with the MSTI using the spanning-tree mst instance command.

Example To associate VLAN 30 with MSTI 2, use the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 2 vlan 30
```

Related Commands

region (MSTP)

revision (MSTP)

show spanning-tree mst config

spanning-tree mst instance

vlan

region (MSTP)

Overview Use this command to assign a name to the device's MST Region. MST Instances (MSTI) of a region form different spanning trees for different VLANs.

Use this command for MSTP only.

Use the **no** variant of this command to remove this region name and reset it to the default.

Syntax

```
region <region-name>
no region
```

Parameter	Description
<region-name>	Specify the name of the region, up to 32 characters. Valid characters are upper-case, lower-case, digits, underscore.

Default By default, the region name is My Name.

Mode MST Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# region ATL
```

Related Commands revision (MSTP)

show spanning-tree mst config

revision (MSTP)

Overview Use this command to specify the MST revision number to be used in the configuration identifier.

Use this command for MSTP only.

Syntax

```
revision <revision-number>
```

Parameter	Description
<revision-number>	<0-65535> Revision number.

Default The default of revision number is 0.

Mode MST Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# revision 25
```

Related Commands

region (MSTP)

show spanning-tree mst config

instance vlan (MSTP)

show debugging mstp

Overview Use this command to show the MSTP debugging options set.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging mstp
```

Mode User Exec and Privileged Exec mode

Example To display the MSTP debugging options set, enter the command:

```
awplus# show debugging mstp
```

Output Figure 14-1: Example output from **show debugging mstp**

```
MSTP debugging status:
  MSTP receiving packet debugging is on
```

Related Commands debug mstp (RSTP and STP)

show spanning-tree

Overview Use this command to display detailed spanning tree information on the specified port or on all ports. Use this command for RSTP, MSTP or STP.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree [interface <port-list>]
```

Parameter	Description
`interface`	Display information about the following port only.
`<port-list>`	The ports to display information about. A port-list can be: • a switch port (e.g. `port1.0.6`) a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix switch ports, static channel groups, and dynamic (LACP) channel groups in the same list

Mode User Exec and Privileged Exec

Usage Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

Example To display spanning tree information about `port1.0.3`, use the command:

```
awplus# show spanning-tree interface port1.0.3
```

Output Figure 14-2: Example output from **show spanning-tree** in RSTP mode

```
awplus#show spanning-tree
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd24ff2d
% 1: Bridge Id 80000000cd24ff2d
% 1: last topology change Thu Jul 26 02:06:26 2007
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
%   port1.0.1: Designated Path Cost 0
%   port1.0.1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8389 - Priority 128  -
%   port1.0.1: Root 80000000cd24ff2d
%   port1.0.1: Designated Bridge 80000000cd24ff2d
%   port1.0.1: Message Age 0 - Max Age 20
%   port1.0.1: Hello Time 2 - Forward Delay 15
%   port1.0.1: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.0.1: forward-transitions 0
%   port1.0.1: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   port1.0.1: No portfast configured - Current  portfast off
%   port1.0.1: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.1: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.1: no root guard configured     - Current root guard off
%   port1.0.1: Configured Link Type point-to-point - Current  shared
%
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.2: Designated Port Id 838a - Priority 128  -
%   port1.0.2: Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo change
timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Rapid Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
```

Output Figure 14-3: Example output from **show spanning-tree**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: Root Path Cost 0 - Root Port 0 -  Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20
% 1: Root Id 80000000cd20f093
% 1: Bridge Id 80000000cd20f093
% 1: last topology change Sun Nov 20 12:24:24 1977
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.3: Port 5023 - Id 839f - Role Designated - State Forwarding
%   port1.0.3: Designated Path Cost 0
%   port1.0.3: Configured Path Cost 200000  - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 839f - Priority 128  -
%   port1.0.3: Root 80000000cd20f093
%   port1.0.3: Designated Bridge 80000000cd20f093
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: Hello Time 2 - Forward Delay 15
%   port1.0.3: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 1 - topo change
timer 0
%   port1.0.3: forward-transitions 32
%   port1.0.3: Version Rapid Spanning Tree Protocol - Received None - Send RSTP
%   port1.0.3: No portfast configured - Current  portfast off
%   port1.0.3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured     - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current point-to-point
...
```

show spanning-tree brief

Overview Use this command to display a summary of spanning tree status information on all ports. Use this command for RSTP, MSTP or STP.

Syntax

```
show spanning-tree brief
```

Parameter	Description
`brief`	A brief summary of spanning tree information.

Mode User Exec and Privileged Exec

Usage Note that any list of interfaces specified must not span any interfaces that are not installed.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the **show spanning-tree** command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

Example To display a summary of spanning tree status information, use the command:

```
awplus# show spanning-tree brief
```

Output Figure 14-4: Example output from **show spanning-tree brief**

```
Default: Bridge up - Spanning Tree Enabled
Default: Root Path Cost 40000 - Root Port 4501 -  Bridge Priority 32768
Default: Root Id 8000:0000cd250001
Default: Bridge Id 8000:0000cd296eb1

Port            Designated Bridge    Port Id    Role          State
sa1             8000:001577c9744b    8195       Rootport      Forwarding
po1             8000:0000cd296eb1    81f9       Designated    Forwarding
port1.0.1       8000:0000cd296eb1    8389       Disabled      Discarding
port1.0.2       8000:0000cd296eb1    838a       Disabled      Discarding
port1.0.3       8000:0000cd296eb1    838b       Disabled      Discarding
...
```

Related Commands show spanning-tree

show spanning-tree mst

Overview This command displays bridge-level information about the CIST and VLAN to MSTI mappings.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst
```

Mode User Exec, Privileged Exec and Interface Configuration

Example To display bridge-level information about the CIST and VLAN to MSTI mappings, enter the command:

```
awplus# show spanning-tree mst
```

Output Figure 14-5: Example output from **show spanning-tree mst**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge
Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 8000000475e93ffe
% 1: CIST Reg Root Id 8000000475e93ffe
% 1: CST Bridge Id 8000000475e93ffe
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%
%   Instance        VLAN
%   0:              1
%   2:              4
```

Related Commands show spanning-tree mst interface

show spanning-tree mst config

Overview Use this command to display MSTP configuration identifier for the device.

Syntax

```
show spanning-tree mst config
```

Mode User Exec, Privileged Exec and Interface Configuration

Usage The region name, the revision number, and the digest of the VLAN to MSTI configuration table must be the same on all devices that are intended to be in the same MST region.

Example To display MSTP configuration identifier information, enter the command:

```
awplus# show spanning-tree mst config
```

Output Figure 14-6: Example output from **show spanning-tree mst config**

```
awplus#show spanning-tree mst config
%
%  MSTP Configuration Information:
%--------------------------------------------------------
%  Format Id      : 0
%  Name           : My Name
%  Revision Level : 0
%  Digest         : 0x80DEE46DA92A98CF21C603291B22880A
%--------------------------------------------------------
```

Related Commands

instance vlan (MSTP)

region (MSTP)

revision (MSTP)

show spanning-tree mst detail

Overview This command displays detailed information about each instance, and all interfaces associated with that particular instance.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst detail
```

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about each instance, and all interfaces associated with them, enter the command:

```
awplus# show spanning-tree mst detail
```

Output Figure 14-7: Example output from **show spanning-tree mst detail**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.1: Port 5001 - Id 8389 - Role Disabled - State Discarding
%   port1.0.1: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.1: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.1: Designated Port Id 8389 - CIST Priority 128  -
%   port1.0.1: CIST Root 80000000cd24ff2d
%   port1.0.1: Regional Root 80000000cd24ff2d
%   port1.0.1: Designated Bridge 80000000cd24ff2d
%   port1.0.1: Message Age 0 - Max Age 20
%   port1.0.1: CIST Hello Time 2 - Forward Delay 15
%   port1.0.1: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
...
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
```

```
%   port1.0.3: Port 5003 - Id 838b - Role Disabled - State Discarding
%   port1.0.3: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.3: Configured Path Cost 20000000  - Add type Explicit ref count 1
%   port1.0.3: Designated Port Id 838b - CIST Priority 128  -
%   port1.0.3: CIST Root 80000000cd24ff2d
%   port1.0.3: Regional Root 80000000cd24ff2d
%   port1.0.3: Designated Bridge 80000000cd24ff2d
%   port1.0.3: Message Age 0 - Max Age 20
%   port1.0.3: CIST Hello Time 2 - Forward Delay 15
%   port1.0.3: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.3: forward-transitions 0
%   port1.0.3: Version Multiple Spanning Tree Protocol - Received None - Send STP
%   port1.0.3: No portfast configured - Current  portfast off
%   port1.0.3: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.3: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.3: no root guard configured     - Current root guard off
%   port1.0.3: Configured Link Type point-to-point - Current  shared
```

show spanning-tree mst detail interface

Overview This command displays detailed information about the specified switch port, and the MST instances associated with it.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst detail interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about `port1.0.3` and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

Output Figure 14-8: Example output from **show spanning-tree mst detail interface**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 2
%   port1.0.2: Designated Port Id 838a - CIST Priority 128  -
%   port1.0.2: CIST Root 80000000cd24ff2d
%   port1.0.2: Regional Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: CIST Hello Time 2 - Forward Delay 15
%   port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
```

```
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
% Instance  2:  Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

show spanning-tree mst instance

Overview This command displays detailed information for the specified instance, and all switch ports associated with that instance.

A topology change counter has been included for RSTP and MSTP. You can see the topology change counter for RSTP by using the show spanning-tree command. You can see the topology change counter for MSTP by using the **show spanning-tree mst instance** command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst instance <instance-id>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.

Mode User Exec, Privileged Exec, and Interface Configuration

Usage To display detailed information for **instance 2**, and all switch ports associated with that instance, use the command:

```
awplus# show spanning-tree mst instance 2
```

Output Figure 14-9: Example output from **show spanning-tree mst instance**

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

show spanning-tree mst instance interface

Overview This command displays detailed information for the specified MST (Multiple Spanning Tree) instance, and the specified switch port associated with that MST instance.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst instance <instance-id> interface <port>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information for `instance 2`, interface `port1.0.2`, use the command:

```
awplus# show spanning-tree mst instance 2 interface port1.0.2
```

Output Figure 14-10: Example output from **show spanning-tree mst instance**

```
% 1: MSTI Root Path Cost 0 - MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
%
```

show spanning-tree mst interface

Overview This command displays the number of instances created, and VLANs associated with it for the specified switch port.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec, and Interface Configuration

Example To display detailed information about each instance, and all interfaces associated with them, for `port1.0.4`, use the command:

```
awplus# show spanning-tree mst interface port1.0.4
```

Output Figure 14-11: Example output from **show spanning-tree mst interface**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 - CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000008c73a2b22
% 1: CIST Reg Root Id 80000008c73a2b22
% 1: CST Bridge Id 80000008c73a2b22
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 1 sec
%
%   Instance        VLAN
%   0:              1
%   1:              2-3
%   2:              4-5
```

show spanning-tree mst detail interface

Overview This command displays detailed information about the specified switch port, and the MST instances associated with it.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree mst detail interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode User Exec, Privileged Exec and Interface Configuration

Example To display detailed information about `port1.0.3` and the instances associated with it, enter the command:

```
awplus# show spanning-tree mst detail interface port1.0.3
```

Output Figure 14-12: Example output from **show spanning-tree mst detail interface**

```
% 1: Bridge up - Spanning Tree Enabled
% 1: CIST Root Path Cost 0 - CIST Root Port 0 -  CIST Bridge Priority 32768
% 1: Forward Delay 15 - Hello Time 2 - Max Age 20 - Max-hops 20
% 1: CIST Root Id 80000000cd24ff2d
% 1: CIST Reg Root Id 80000000cd24ff2d
% 1: CIST Bridge Id 80000000cd24ff2d
% 1: portfast bpdu-filter disabled
% 1: portfast bpdu-guard disabled
% 1: portfast errdisable timeout disabled
% 1: portfast errdisable timeout interval 300 sec
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated External Path Cost 0 -Internal Path Cost 0
%   port1.0.2: Configured Path Cost 20000000  - Add type Explicit ref count 2
%   port1.0.2: Designated Port Id 838a - CIST Priority 128  -
%   port1.0.2: CIST Root 80000000cd24ff2d
%   port1.0.2: Regional Root 80000000cd24ff2d
%   port1.0.2: Designated Bridge 80000000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 20
%   port1.0.2: CIST Hello Time 2 - Forward Delay 15
%   port1.0.2: CIST Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0 - topo
change timer 0
%   port1.0.2: forward-transitions 0
%   port1.0.2: Version Multiple Spanning Tree Protocol - Received None - Send STP
```

```
%   port1.0.2: No portfast configured - Current  portfast off
%   port1.0.2: portfast bpdu-guard  default  - Current portfast bpdu-guard off
%   port1.0.2: portfast bpdu-filter default  - Current portfast bpdu-filter off
%   port1.0.2: no root guard configured     - Current root guard off
%   port1.0.2: Configured Link Type point-to-point - Current  shared
%
% Instance  2:  Vlans: 2
% 1: MSTI Root Path Cost 0 -MSTI Root Port 0 - MSTI Bridge Priority 32768
% 1: MSTI Root Id 80020000cd24ff2d
% 1: MSTI Bridge Id 80020000cd24ff2d
%   port1.0.2: Port 5002 - Id 838a - Role Disabled - State Discarding
%   port1.0.2: Designated Internal Path Cost 0  - Designated Port Id 838a
%   port1.0.2: Configured Internal Path Cost 20000000
%   port1.0.2: Configured CST External Path cost 20000000
%   port1.0.2: CST Priority 128  - MSTI Priority 128
%   port1.0.2: Designated Root 80020000cd24ff2d
%   port1.0.2: Designated Bridge 80020000cd24ff2d
%   port1.0.2: Message Age 0 - Max Age 0
%   port1.0.2: Hello Time 2 - Forward Delay 15
%   port1.0.2: Forward Timer 0 - Msg Age Timer 0 - Hello Timer 0
```

show spanning-tree statistics

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show spanning-tree statistics
```

Mode Privileged Exec

Usage To display BPDU statistics for all spanning-tree instances, and all switch ports associated with all spanning-tree instances, use the command:

```
awplus# show spanning-tree statistics
```

Output Figure 14-13: Example output from **show spanning-tree statistics**

```
Port number = 915 Interface = port1.0.6
                ================================
% BPDU Related Parameters
% ----------------------
% Port Spanning Tree                : Disable
% Spanning Tree Type                : Rapid Spanning Tree Protocol
% Current Port State                : Discarding
% Port ID                           : 8393
% Port Number                       : 393
% Path Cost                         : 20000000
% Message Age                       : 0
% Designated Root                   : ec:cd:6d:20:c0:ed
% Designated Cost                   : 0
% Designated Bridge                 : ec:cd:6d:20:c0:ed
% Designated Port Id                : 8393
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE
% PORT Based Information & Statistics
% ----------------------------------
% Config Bpdu's xmitted             : 0
% Config Bpdu's received            : 0
% TCN Bpdu's xmitted                : 0
% TCN Bpdu's received               : 0
% Forward Trans Count               : 0
```

```
% STATUS of Port Timers
% ----------------------
% Hello Time Configured              : 2
% Hello timer                        : INACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0
% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 0
% Next State                         : Learning
% Topology Change Time               : 0
```

show spanning-tree statistics instance

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance, and all switch ports associated with that MST instance.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree statistics instance <instance-id>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.

Mode Privileged Exec

Usage To display BPDU statistics information for MST instance 2, and all switch ports associated with that MST instance, use the command:

```
awplus# show spanning-tree statistics instance 2
```

Output Figure 14-14: Example output from **show spanning-tree statistics instance**

```
% % INST_PORT port1.0.3 Information & Statistics
% ----------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.3: Forward Transitions                : 0
% Next State                           : Learning
% Topology Change Time                 : 0
...
```

Related Commands show spanning-tree statistics

show spanning-tree statistics instance interface

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified MST (Multiple Spanning Tree) instance and the specified switch port associated with that MST instance.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree statistics instance <instance-id> interface
<port>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example To display BPDU statistics for MST `instance 2`, interface `port1.0.2`, use the command:

```
awplus# show spanning-tree statistics instance 2 interface
port1.0.2
```

Output Figure 14-15: Example output from **show spanning-tree statistics instance interface**

```
awplus#sh spanning-tree statistics interface port1.0.2 instance 1
        Spanning Tree Enabled for Instance : 1
        ==================================
% INST_PORT port1.0.2 Information & Statistics
% -------------------------------------
% Config Bpdu's xmitted (port/inst)    : (0/0)
% Config Bpdu's received (port/inst)   : (0/0)
% TCN Bpdu's xmitted (port/inst)       : (0/0)
% TCN Bpdu's received (port/inst)      : (0/0)
% Message Age(port/Inst)               : (0/0)
% port1.0.2: Forward Transitions                 : 0
% Next State                           : Learning
% Topology Change Time                 : 0

% Other Inst/Vlan Information & Statistics
% -------------------------------------
% Bridge Priority                     : 0
% Bridge Mac Address                  : ec:cd:6d:20:c0:ed
% Topology Change Initiator           : 5023
% Last Topology Change Occured        : Mon Aug 22 05:42:06 2011
% Topology Change                     : FALSE
% Topology Change Detected            : FALSE
% Topology Change Count               : 1
% Topology Change Last Recvd from     : 00:00:00:00:00:00
```

Related Commands show spanning-tree statistics

show spanning-tree statistics interface

Overview This command displays BPDU (Bridge Protocol Data Unit) statistics for the specified switch port, and all MST instances associated with that switch port.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show spanning-tree statistics interface <port>
```

Parameter	Description
<port>	The port to display information about. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Privileged Exec

Example To display BPDU statistics about each MST instance for `port1.0.4`, use the command:

```
awplus# show spanning-tree statistics interface port1.0.4
```

Output Figure 14-16: Example output from **show spanning-tree statistics interface**

```
awplus#show spanning-tree statistics interface port1.0.2

              Port number = 906 Interface = port1.0.2
                ================================
% BPDU Related Parameters
% ------------------------
% Port Spanning Tree                : Disable
% Spanning Tree Type                : Multiple Spanning Tree Protocol
% Current Port State                : Discarding
% Port ID                           : 838a
% Port Number                       : 38a
% Path Cost                         : 20000000
% Message Age                       : 0
% Designated Root                   : ec:cd:6d:20:c0:ed
% Designated Cost                   : 0
% Designated Bridge                 : ec:cd:6d:20:c0:ed
% Designated Port Id                : 838a
% Top Change Ack                    : FALSE
% Config Pending                    : FALSE
```

```
% PORT Based Information & Statistics
% -----------------------------------
% Config Bpdu's xmitted              : 0
% Config Bpdu's received             : 0
% TCN Bpdu's xmitted                 : 0
% TCN Bpdu's received                : 0
% Forward Trans Count                : 0

% STATUS of Port Timers
% ---------------------
% Hello Time Configured              : 2
% Hello timer                        : INACTIVE
% Hello Time Value                   : 0
% Forward Delay Timer                : INACTIVE
% Forward Delay Timer Value          : 0
% Message Age Timer                  : INACTIVE
% Message Age Timer Value            : 0
% Topology Change Timer              : INACTIVE
% Topology Change Timer Value        : 0
% Hold Timer                         : INACTIVE
% Hold Timer Value                   : 0

% Other Port-Specific Info
  ------------------------
% Max Age Transitions                : 1
% Msg Age Expiry                     : 0
% Similar BPDUS Rcvd                 : 0
% Src Mac Count                      : 0
% Total Src Mac Rcvd                 : 0
% Next State                         : Learning
% Topology Change Time               : 0
% Other Bridge information & Statistics
  -------------------------------------
% STP Multicast Address              : 01:80:c2:00:00:00
% Bridge Priority                    : 32768
% Bridge Mac Address                 : ec:cd:6d:20:c0:ed
% Bridge Hello Time                  : 2
% Bridge Forward Delay               : 15
% Topology Change Initiator          : 5023
% Last Topology Change Occured       : Mon Aug 22 05:41:20 2011
% Topology Change                    : FALSE
% Topology Change Detected           : TRUE
% Topology Change Count              : 1
% Topology Change Last Recvd from    : 00:00:00:00:00:00
```

Related Commands show spanning-tree statistics

show spanning-tree vlan range-index

Overview Use this command to display information about MST (Multiple Spanning Tree) instances and the VLANs associated with them including the VLAN range-index value for the device.

Syntax

```
show spanning-tree vlan range-index
```

Mode Privileged Exec

Example To display information about MST instances and the VLANs associated with them for the device, including the VLAN range-index value, use the following command:

```
awplus# show spanning-tree vlan range-index
```

Output Figure 14-17: Example output from **show spanning-tree vlan range-index**

```
awplus#show spanning-tree vlan range-index
% MST Instance  VLAN       RangeIdx
%      1        1          1%
```

Related Commands show spanning-tree statistics

spanning-tree autoedge (RSTP and MSTP)

Overview Use this command to enable the autoedge feature on the port.

The autoedge feature allows the port to automatically detect that it is an edge port. If it does not receive any BPDUs in the first three seconds after linkup, enabling, or entering RSTP or MSTP mode, it sets itself to be an edgeport and enters the forwarding state.

Use this command for RSTP or MSTP.

Use the **no** variant of this command to disable this feature.

Syntax

```
spanning-tree autoedge
no spanning-tree autoedge
```

Default Disabled

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# spanning-tree autoedge
```

Related Commands spanning-tree edgeport (RSTP and MSTP)

spanning-tree bpdu

Overview Use this command in Global Configuration mode to configure BPDU (Bridge Protocol Data Unit) discarding or forwarding, with STP (Spanning Tree Protocol) disabled on the switch.

See the Usage note about disabling Spanning Tree before using this command, and using this command to forward unsupported BPDUs unchanged for unsupported STP Protocols.

There is not a **no** variant for this command. Instead, apply the `discard` parameter to reset it back to the default then re-enable STP with **spanning-tree enable** command.

Syntax

```
spanning-tree bpdu
{discard|forward|forward-untagged-vlan|forward-vlan}
```

Parameter	Description	
`bpdu`	A port that has BPDU filtering enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Global Configuration mode):	
	`discard`	Discards all ingress STP BPDU frames.
	`forward`	Forwards any ingress STP BPDU packets to all ports, regardless of any VLAN membership.
	`forward-untagged-vlan`	Forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN.
	`forward-vlan`	Forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN.

Default The discard parameter is enabled by default.

Mode Global Configuration

Usage You must first disable Spanning Tree with the spanning-tree enable command before you can use this command to then configure BPDU discarding or forwarding.

This command enables the switch to forward unsupported BPDUs with an unsupported Spanning Tree Protocol, such as proprietary STP protocols with unsupported BPDUs, by forwarding BDPU (Bridge Protocol Data Unit) frames unchanged through the switch.

When you want to revert to default behavior on the switch, issue a **spanning-tree bdpu discard** command and re-enable Spanning Tree with a **s panning-tree enable** command.

Examples

To enable STP BPDU discard in Global Configuration mode with STP disabled, which discards all ingress STP BPDU frames, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu discard
```

To enable STP BPDU forward in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports regardless of any VLAN membership, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward
```

To enable STP BPDU forwarding for untagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are untagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-untagged-vlan
```

To enable STP BPDU forwarding for tagged frames in Global Configuration mode with STP disabled, which forwards any ingress STP BPDU frames to all ports that are tagged members of the ingress port's native VLAN, enter the commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
awplus(config)# spanning-tree bpdu forward-vlan
```

To reset STP BPDU back to the default `discard` parameter and re-enable STP on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree bpdu discard
awplus(config)# spanning-tree stp enable
```

Related Commands

show spanning-tree

spanning-tree enable

spanning-tree cisco-interoperability (MSTP)

Overview Use this command to enable/disable Cisco-interoperability for MSTP.

Use this command for MSTP only.

Syntax

```
spanning-tree cisco-interoperability {enable|disable}
```

Parameter	Description
`enable`	Enable Cisco interoperability for MSTP.
`disable`	Disable Cisco interoperability for MSTP.

Default If this command is not used, Cisco interoperability is disabled.

Mode Global Configuration

Usage For compatibility with certain Cisco devices, all devices in the switched LAN running the AlliedWare Plus™ Operating System must have Cisco-interoperability enabled. When the AlliedWare Plus Operating System is interoperating with Cisco, the only criteria used to classify a region are the region name and revision level. VLAN to instance mapping is not used to classify regions when interoperating with Cisco.

Examples To enable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability enable
```

To disable Cisco interoperability on a Layer 2 device:

```
awplus# configure terminal
awplus(config)# spanning-tree cisco-interoperability disable
```

spanning-tree edgeport (RSTP and MSTP)

Overview Use this command to set a port as an edge-port.

Use this command for RSTP or MSTP.

This command has the same effect as the spanning-tree portfast (STP) command, but the configuration displays differently in the output of some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

Syntax
```
spanning-tree edgeport
no spanning-tree edgeport
```

Default Not an edge port.

Mode Interface Configuration

Usage Use this command on a switch port connected to a LAN that has no other bridges attached. If a BPDU is received on the port that indicates that another bridge is connected to the LAN, then the port is no longer treated as an edge port.

Example
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree edgeport
```

Related Commands spanning-tree autoedge (RSTP and MSTP)

spanning-tree enable

Overview Use this command in Global Configuration mode to enable the specified spanning tree protocol for all switch ports. Note that this must be the spanning tree protocol that is configured on the device by the spanning-tree mode command.

Use the **no** variant of this command to disable the configured spanning tree protocol. This places all switch ports in the forwarding state.

Syntax

```
spanning-tree {mstp|rstp|stp} enable
no spanning-tree {mstp|rstp|stp} enable
```

Parameter	Description
`mstp`	Enables or disables MSTP (Multiple Spanning Tree Protocol).
`rstp`	Enables or disables RSTP (Rapid Spanning Tree Protocol).
`stp`	Enables or disables STP (Spanning Tree Protocol).

Default RSTP is enabled by default for all switch ports.

Mode Global Configuration

Usage With no configuration, spanning tree is enabled, and the spanning tree mode is set to RSTP. To change the mode, see spanning-tree mode command.

Examples To enable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

To disable STP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree stp enable
```

To enable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mstp enable
```

To disable MSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree mstp enable
```

To enable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

To disable RSTP in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable
```

Related Commands

spanning-tree bpdu

spanning-tree mode

spanning-tree errdisable-timeout enable

Overview Use this command to enable the errdisable-timeout facility, which sets a timeout for ports that are disabled due to the BPDU guard feature.

Use this command for RSTP or MSTP.

Use the **no** variant of this command to disable the errdisable-timeout facility.

Syntax
```
spanning-tree errdisable-timeout enable
no spanning-tree errdisable-timeout enable
```

Default By default, the errdisable-timeout is disabled.

Mode Global Configuration

Usage The BPDU guard feature shuts down the port on receiving a BPDU on a BPDU-guard enabled port. This command associates a timer with the feature such that the port is re- enabled without manual intervention after a set interval. This interval can be configured by the user using the spanning-tree errdisable-timeout interval command.

Example
```
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout enable
```

Related Commands
show spanning-tree

spanning-tree errdisable-timeout interval

spanning-tree portfast bpdu-guard

spanning-tree errdisable-timeout interval

Overview Use this command to specify the time interval after which a port is brought back up when it has been disabled by the BPDU guard feature.

Use this command for RSTP or MSTP.

Syntax

```
spanning-tree errdisable-timeout interval <10-1000000>
no spanning-tree errdisable-timeout interval
```

Parameter	Description
<10-1000000>	Specify the errdisable-timeout interval in seconds.

Default By default, the port is re-enabled after 300 seconds.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# spanning-tree errdisable-timeout interval 34
```

Related Commands

show spanning-tree

spanning-tree errdisable-timeout enable

spanning-tree portfast bpdu-guard

spanning-tree force-version

Overview Use this command in Interface Configuration mode for a switch port interface only to force the protocol version for the switch port. Use this command for RSTP or MSTP only.

Syntax

```
spanning-tree force-version <version>
no spanning-tree force-version
```

Parameter	Description	
<version>	<0-3> Version identifier.	
	0	Forces the port to operate in STP mode.
	1	Not supported.
	2	Forces the port to operate in RSTP mode. If it receives STP BPDUs, it can automatically revert to STP mode.
	3	Forces the port to operate in MSTP mode (this option is only available if MSTP mode is configured). If it receives RSTP or STP BPDUs, it can automatically revert to RSTP or STP mode.

Default By default, no version is forced for the port. The port is in the spanning tree mode configured for the device, or a lower version if it automatically detects one.

Mode Interface Configuration mode for a switch port interface only.

Examples Set the value to enforce the spanning tree protocol (STP):

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree force-version 0
```

Set the default protocol version:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree force-version
```

Related Commands show spanning-tree

spanning-tree forward-time

Overview Use this command to set the forward delay value. Use the **no** variant of this command to reset the forward delay value to the default setting of 15 seconds.

The **forward delay** sets the time (in seconds) to control how fast a port changes its spanning tree state when moving towards the forwarding state. If the mode is set to STP, the value determines how long the port stays in each of the listening and learning states which precede the forwarding state. If the mode is set to RSTP or MSTP, this value determines the maximum time taken to transition from discarding to learning and from learning to forwarding.

This value is used only when the device is acting as the root bridge. Devices not acting as the Root Bridge use a dynamic value for the **forward delay** set by the root bridge. The **forward delay**, **max-age**, and **hello time** parameters are interrelated.

Syntax

```
spanning-tree forward-time <forward-delay>
no spanning-tree forward-time
```

Parameter	Description
<forward-delay>	<4-30> The forwarding time delay in seconds.

Default The default is 15 seconds.

Mode Global Configuration

Usage The allowable range for forward-time is 4-30 seconds.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age >= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree forward-time 6
```

Related Commands

show spanning-tree

spanning-tree forward-time

spanning-tree hello-time

spanning-tree mode

spanning-tree guard root

Overview Use this command in Interface Configuration mode for a switch port only to enable the Root Guard feature for the switch port. The root guard feature disables reception of superior BPDUs. You can use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to disable the root guard feature for the port.

Syntax

```
spanning-tree guard root
no spanning-tree guard root
```

Mode Interface Configuration mode for a switch port interface only.

Usage The Root Guard feature makes sure that the port on which it is enabled is a designated port. If the Root Guard enabled port receives a superior BPDU, it goes to a Listening state (for STP) or discarding state (for RSTP and MSTP).

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree guard root
```

spanning-tree hello-time

Overview Use this command to set the hello-time. This sets the time in seconds between the transmission of device spanning tree configuration information when the device is the Root Bridge of the spanning tree or is trying to become the Root Bridge.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of the hello time.

Syntax

```
spanning-tree hello-time <hello-time>
no spanning-tree hello-time
```

Parameter	Description
<hello-time>	<1-10> The hello BPDU interval in seconds.

Default Default is 2 seconds.

Mode Global Configuration and Interface Configuration for switch ports.

Usage The allowable range of values is 1-10 seconds.

The forward delay, max-age, and hello time parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age>= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree hello-time 3
```

Related Commands

spanning-tree forward-time

spanning-tree max-age

show spanning-tree

spanning-tree link-type

Overview Use this command in Interface Configuration mode for a switch port interface only to enable or disable point-to-point or shared link types on the switch port.

Use this command for RSTP or MSTP only.

Use the **no** variant of this command to return the port to the default link type.

Syntax

```
spanning-tree link-type {point-to-point|shared}
no spanning-tree link-type
```

Parameter	Description
`shared`	Disable rapid transition.
`point-to-point`	Enable rapid transition.

Default The default link type is point-to-point.

Mode Interface Configuration mode for a switch port interface only.

Usage You may want to set link type to shared if the port is connected to a hub with multiple devices connected to it.

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree link-type point-to-point
```

spanning-tree max-age

Overview Use this command to set the max-age. This sets the maximum age, in seconds, that dynamic spanning tree configuration information is stored in the device before it is discarded.

Use this command for RSTP, STP or MSTP.

Use the **no** variant of this command to restore the default of max-age.

Syntax

```
spanning-tree max-age <max-age>
no spanning-tree max-age
```

Parameter	Description
<max-age>	<6-40> The maximum time, in seconds.

Default The default of spanning-tree max-age is 20 seconds.

Mode Global Configuration

Usage Max-age is the maximum time in seconds for which a message is considered valid.

Configure this value sufficiently high, so that a frame generated by the root bridge can be propagated to the leaf nodes without exceeding the max-age.

The **forward delay**, **max-age**, and **hello time** parameters should be set according to the following formula, as specified in IEEE Standard 802.1d:

2 x (forward delay - 1.0 seconds) >= max-age

max-age >= 2 x (hello time + 1.0 seconds)

Example

```
awplus# configure terminal
awplus(config)# spanning-tree max-age 12
```

Related Commands

show spanning-tree

spanning-tree forward-time

spanning-tree hello-time

spanning-tree max-hops (MSTP)

Overview Use this command to specify the maximum allowed hops for a BPDU in an MST region. This parameter is used by all the instances of the MST region.

Use the **no** variant of this command to restore the default.

Use this command for MSTP only.

Syntax

```
spanning-tree max-hops <hop-count>
no spanning-tree max-hops <hop-count>
```

Parameter	Description
<hop-count>	Specify the maximum hops the BPDU will be valid for in the range <1-40>.

Default The default max-hops in a MST region is 20.

Mode Global Configuration

Usage Specifying the max hops for a BPDU prevents the messages from looping indefinitely in the network. The hop count is decremented by each receiving port. When a device receives an MST BPDU that has a hop count of zero, it discards the BPDU.

Examples

```
awplus# configure terminal
awplus(config)# spanning-tree max-hops 25
awplus# configure terminal
awplus(config)# no spanning-tree max-hops
```

spanning-tree mode

Overview Use this command to change the spanning tree protocol mode on the device. The spanning tree protocol mode on the device can be configured to either STP, RSTP or MSTP.

Syntax

```
spanning-tree mode {stp|rstp|mstp}
```

Default The default spanning tree protocol mode on the device is RSTP.

Mode Global Configuration

Usage With no configuration, the device will have spanning tree enabled, and the spanning tree mode will be set to RSTP. Use this command to change the spanning tree protocol mode on the device. MSTP is VLAN aware, but RSTP and STP are not VLAN aware. To enable or disable spanning tree operation, see the spanning-tree enable command.

Examples To change the spanning tree mode from the default of RSTP to MSTP, use the following commands:

```
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
```

Related Commands spanning-tree enable

spanning-tree mst configuration

Overview Use this command to enter the MST Configuration mode to configure the Multiple Spanning-Tree Protocol.

Syntax

```
spanning-tree mst configuration
```

Mode Global Configuration

Examples The following example uses this command to enter MST Configuration mode. Note the change in the command prompt.

```
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)#
```

spanning-tree mst instance

Overview Use this command to assign a Multiple Spanning Tree instance (MSTI) to a switch port or channel group.

Note that ports are automatically configured to send and receive spanning-tree information for the associated MSTI when VLANs are assigned to MSTIs using the instance vlan (MSTP) command.

Use the **no** variant of this command in Interface Configuration mode to remove the MSTI from the specified switch port or channel group.

Syntax

```
spanning-tree mst instance <instance-id>
no spanning-tree mst instance <instance-id>
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15. The MST instance must have already been created using the instance vlan (MSTP) command.

Default A port automatically becomes a member of an MSTI when it is assigned to a VLAN.

Mode Interface Configuration mode for a switch port or channel group.

Usage You can disable automatic configuration of member ports of a VLAN to an associated MSTI by using a **no spanning-tree mst instance** command to remove the member port from the MSTI. Use the **spanning-tree mst instance** command to add a VLAN member port back to the MSTI.

Examples To assign instance 3 to a switch port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3
```

To remove instance 3 from a switch port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
```

Related Commands

instance vlan (MSTP)

spanning-tree mst instance path-cost

spanning-tree mst instance priority

spanning-tree mst instance restricted-role

spanning-tree mst instance restricted-tcn

spanning-tree mst instance path-cost

Overview Use this command to set the cost of a path associated with a switch port, for the specified MSTI.

This specifies the switch port's contribution to the cost of a path to the MSTI regional root via that port. This applies when the port is the root port for the MSTI.

Use the **no** variant of this command to restore the default cost value of the path.

Syntax

```
spanning-tree mst instance <instance-id> path-cost <path-cost>
no spanning-tree mst instance <instance-id> path-cost
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<path-cost>	Specify the cost of path in the range of <1-200000000>, where a lower path-cost indicates a greater likelihood of the specific interface becoming a root.

Default The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 standard.

Port speed	Default path cost	Recommended path cost range
Less than 100 Kb/s	200,000,000	20,000,000-200,000,000
1Mbps	20,000,000	2,000,000-20,000,000
10Mbps	2,000,000	200,000-2,000,000
100 Mbps	200,000	20,000-200,000
1 Gbps	20,000	2,000-20,000
10 Gbps	2,000	200-2, 000
100 Gbps	200	20-200
1Tbps	20	2-200
10 Tbps	2	2-20

Mode Interface Configuration mode for a switch port interface only.

Usage Before you can use this command to set a path-cost in a VLAN configuration, you must explicitly add an MST instance to a port using the spanning-tree mst instance command.

Examples To set a path cost of 1000 on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 path-cost 1000
```

To return the path cost to its default value on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 path-cost
```

Related Commands

instance vlan (MSTP)

spanning-tree mst instance

spanning-tree mst instance priority

spanning-tree mst instance restricted-role

spanning-tree mst instance restricted-tcn

spanning-tree mst instance priority

Overview Use this command in Interface Configuration mode for a switch port interface only to set the port priority for an MST instance (MSTI).

Use the **no** variant of this command to restore the default priority value (128).

Syntax

```
spanning-tree mst instance <instance-id> priority <priority>
no spanning-tree mst instance <instance-id> [priority]
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15.
<priority>	This must be a multiple of 16 and within the range <0-240>. A lower priority indicates greater likelihood of the port becoming the root port.

Default The default is 128.

Mode Interface Configuration mode for a switch port interface.

Usage This command sets the value of the priority field contained in the port identifier. The MST algorithm uses the port priority when determining the root port for the switch in the MSTI. The port with the lowest value has the highest priority, so it will be chosen as root port over a port that is equivalent in all other aspects but with a higher priority value.

Examples To set the priority to 112 on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 priority 112
```

To return the priority to its default value of 128 on instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3 priority
```

Related Commands

instance vlan (MSTP)

spanning-tree priority (port priority)

spanning-tree mst instance

spanning-tree mst instance path-cost

spanning-tree mst instance restricted-role

spanning-tree mst instance restricted-tcn

spanning-tree mst instance restricted-role

Overview Use this command in Interface Configuration mode for a switch port interface only to enable the restricted role for an MSTI (Multiple Spanning Tree Instance) on a switch port. Configuring the restricted role for an MSTI on a switch port prevents the switch port from becoming the root port in a spanning tree topology.

Use the **no** variant of this command to disable the restricted role for an MSTI on a switch port. Removing the restricted role for an MSTI on a switch port allows the switch port to become the root port in a spanning tree topology.

Syntax

```
spanning-tree mst instance <instance-id> restricted-role
no spanning-tree mst instance <instance-id> restricted-role
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15. The MST instance must have already been created using the instance vlan (MSTP) command.

Default The restricted role for an MSTI instance on a switch port is disabled by default.

Mode Interface Configuration mode for a switch port interface only.

Usage The root port is the port providing the best path from the bridge to the root bridge. Use this command to disable a port from becoming a root port. Use the **no** variant of this command to enable a port to become a root port. See the STP Feature Overview and Configuration Guide for root port information.

Examples To prevent a switch port from becoming the root port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-role
```

To stop preventing the switch port from becoming the root port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-role
```

Related Commands

instance vlan (MSTP)

spanning-tree priority (port priority)

spanning-tree mst instance

spanning-tree mst instance path-cost

spanning-tree mst instance restricted-tcn

spanning-tree mst instance restricted-tcn

Overview Use this command to prevent a switch port from propagating received topology change notifications and topology changes to other switch ports. This is named restricted TCN (Topology Change Notification). A TCN is a simple Bridge Protocol Data Unit (BPDU) that a bridge sends out to its root port to signal a topology change.

Use the **no** variant of this command to stop preventing the switch port from propagating received topology change notifications and topology changes to other switch ports for the specified MSTI (Multiple Spanning Tree Instance).

The restricted TCN setting applies only to the specified MSTI (Multiple Spanning Tree Instance).

Syntax

```
spanning-tree mst instance <instance-id> restricted-tcn
no spanning-tree mst instance <instance-id> restricted-tcn
```

Parameter	Description
<instance-id>	Specify an MSTP instance in the range 1-15. The MST instance must have already been created using the instance vlan (MSTP) command.

Default Disabled. By default, switch ports propagate TCNs.

Mode Interface Configuration mode for a switch port interface only.

Examples To prevent a switch port from propagating received topology change notifications and topology changes to other switch ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree mst instance 3 restricted-tcn
```

To stop preventing a switch port from propagating received topology change notifications and topology changes to other switch ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no spanning-tree mst instance 3
restricted-tcn
```

Related Commands

instance vlan (MSTP)

spanning-tree priority (port priority)

spanning-tree mst instance

spanning-tree mst instance path-cost

spanning-tree mst instance restricted-role

spanning-tree path-cost

Overview Use this command in Interface Configuration mode for a switch port interface only to set the cost of a path for the specified port. This value then combines with others along the path to the root bridge in order to determine the total cost path value from the particular port, to the root bridge. The lower the numeric value, the higher the priority of the path. This applies when the port is the root port.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the port's path cost for the CIST.

Syntax

```
spanning-tree path-cost <pathcost>
no spanning-tree path-cost
```

Parameter	Description
<pathcost>	<1-200000000> The cost to be assigned to the port.

Default The default path cost values and the range of recommended path cost values depend on the port speed, as shown in the following table from the IEEE 802.1q-2003 and IEEE 802.1d-2004 standards.

Port speed	Default path cost	Recommended path cost range
Less than 100 Kb/s	200,000,000	20,000,000-200,000,000
1Mbps	20,000,000	2,000,000-20,000,000
10Mbps	2,000,000	200,000-2,000,000
100 Mbps	200,000	20,000-200,000
1 Gbps	20,000	2,000-20,000
10 Gbps	2,000	200-2, 000
100 Gbps	200	20-200
1Tbps	20	2-200
10 Tbps	2	2-20

Mode Interface Configuration mode for switch port interface only.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree path-cost 123
```

spanning-tree portfast (STP)

Overview Use this command in Interface Configuration mode for a switch port interface only to set a port as an edge-port. The portfast feature enables a port to rapidly move to the forwarding state, without having first to pass through the intermediate spanning tree states. This command has the same effect as the spanning-tree edgeport (RSTP and MSTP) command, but the configuration displays differently in the output of some show commands.

NOTE: *You can run either of two additional parameters with this command. To simplify the syntax these are documented as separate commands. See the following additional portfast commands:*

- spanning-tree portfast bpdu-filter command
- spanning-tree portfast bpdu-guard command.

You can obtain the same effect by running the spanning-tree edgeport (RSTP and MSTP) command. However, the configuration output may display differently in some show commands.

Use the **no** variant of this command to set a port to its default state (not an edge-port).

Syntax

```
spanning-tree portfast
no spanning-tree portfast
```

Default Not an edge port.

Mode Interface Configuration mode for a switch port interface only.

Usage Portfast makes a port move from a blocking state to a forwarding state, bypassing both listening and learning states. The portfast feature is meant to be used for ports connected to end-user devices. Enabling portfast on ports that are connected to a workstation or server allows devices to connect to the network without waiting for spanning-tree to converge.

For example, you may need hosts to receive a DHCP address quickly and waiting for STP to converge would cause the DHCP request to time out. Ensure you do not use portfast on any ports connected to another device to avoid creating a spanning-tree loop on the network.

Use this command on a switch port that connects to a LAN with no other bridges attached. An edge port should never receive BPDUs. Therefore if an edge port receives a BPDU, the portfast feature takes one of three actions.

- Cease to act as an edge port and pass BPDUs as a member of a spanning tree network (spanning-tree portfast (STP) command disabled).
- Filter out the BPDUs and pass only the data and continue to act as a edge port (spanning-tree portfast bpdu-filter command enabled).
- Block the port to all BPDUs and data (spanning-tree portfast bpdu-guard command enabled).

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast
```

Related Commands

spanning-tree edgeport (RSTP and MSTP)

show spanning-tree

spanning-tree portfast bpdu-filter

spanning-tree portfast bpdu-guard

spanning-tree portfast bpdu-filter

Overview This command sets the bpdu-filter feature and applies a filter to any BPDUs (Bridge Protocol Data Units) received. Enabling this feature ensures that configured ports will not transmit any BPDUs and will ignore (filter out) any BPDUs received. BPDU Filter is not enabled on a port by default.

Using the **no** variant of this command to turn off the bpdu-filter, but retain the port's status as an enabled port. If the port then receives a BPDU it will change its role from an **edge-port** to a **non edge-port**.

Syntax (Global Configuration)

```
spanning-tree portfast bpdu-filter
no spanning-tree portfast bpdu-filter
```

Syntax (Interface Configuration)

```
spanning-tree portfast bpdu-filter {default|disable|enable}
no spanning-tree portfast bpdu-filter
```

Parameter	Description	
`bpdu-filter`	A port that has bpdu-filter enabled will not transmit any BPDUs and will ignore any BPDUs received. This port type has one of the following parameters (in Interface Configuration mode):	
	`default`	Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.
	`disable`	Turns off BPDU filter.
	`enable`	Turns on BPDU filter.

Default BPDU Filter is not enabled on any ports by default.

Mode Global Configuration and Interface Configuration

Usage This command filters the BPDUs and passes only data to continue to act as an edge port. Using this command in Global Configuration mode applies the portfast bpdu-filter feature to all ports on the device. Using it in Interface mode applies the feature to a specific port, or range of ports.The command will operate in both RSTP and MSTP networks.

Use the show spanning-tree command to display status of the bpdu-filter parameter for the switch ports.

Example To enable STP BPDU filtering in Global Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-filter
```

To enable STP BPDU filtering in Interface Configuration mode, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-filter enable
```

Related Commands

spanning-tree edgeport (RSTP and MSTP)

show spanning-tree

spanning-tree portfast (STP)

spanning-tree portfast bpdu-guard

spanning-tree portfast bpdu-guard

Overview This command applies a BPDU (Bridge Protocol Data Unit) guard to the port. A port with the bpdu-guard feature enabled will block all traffic (BPDUs and user data), if it starts receiving BPDUs.

Use this command in Global Configuration mode to apply BPDU guard to all ports on the device. Use this command in Interface mode for an individual interface or a range of interfaces specified. BPDU Guard is not enabled on a port by default.

Use the **no** variant of this command to disable the BPDU Guard feature on a device in Global Configuration mode or to disable the BPDU Guard feature on a port in Interface mode.

Syntax (Global Configuration)

```
spanning-tree portfast bpdu-guard
no spanning-tree portfast bpdu-guard
```

Syntax (Interface Configuration)

```
spanning-tree portfast bpdu-guard {default|disable|enable}
no spanning-tree portfast bpdu-guard
```

Parameter	Description	
`bpdu-guard`	A port that has bpdu-guard turned on will enter the STP blocking state if it receives a BPDU. This port type has one of the following parameters (in Interface Configuration mode):	
	`default`	Takes the setting that has been configured for the whole device, i.e. the setting made from the Global configuration mode.
	`disable`	Turns off BPDU guard.
	`enable`	Turns on BPDU guard and will also set the port as an edge port.

Default BPDU Guard is not enabled on any ports by default.

Mode Global Configuration or Interface Configuration

Usage This command blocks the port(s) to all devices and data when enabled. BPDU Guard is a port-security feature that changes how a portfast-enabled port behaves if it receives a BPDU. When **bpdu-guard** is set, then the port shuts down if it receives a BPDU. It does not process the BPDU as it is considered suspicious. When **bpdu-guard** is not set, then the port will negotiate spanning-tree with the device sending the BPDUs. By default, bpdu- guard is not enabled on a port.

You can configure a port disabled by the bpdu-guard to re-enable itself after a specific time interval. This interval is set with the spanning-tree errdisable-timeout interval command. If you do not use the **errdisable-timeout** feature, then you will need to manually re-enable the port by using the **no shutdown** command.

Use the show spanning-tree command to display the device and port configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of bpdu-guard.

Example

To enable STP BPDU guard in Global Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# spanning-tree portfast bpdu-guard
```

To enable STP BPDU guard in Interface Configuration mode, enter the below commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree portfast bpdu-guard enable
```

Related Commands

spanning-tree edgeport (RSTP and MSTP)

show spanning-tree

spanning-tree portfast (STP)

spanning-tree portfast bpdu-filter

spanning-tree priority (bridge priority)

Overview Use this command to set the bridge priority for the device. A lower priority value indicates a greater likelihood of the device becoming the root bridge.

Use this command for RSTP, STP or MSTP. When MSTP mode is configured, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

Syntax

```
spanning-tree priority <priority>
no spanning-tree priority
```

Parameter	Description
<priority>	<0-61440> The bridge priority, which will be rounded to a multiple of 4096.

Default The default priority is 32678.

Mode Global Configuration

Usage To force a particular device to become the root bridge use a lower value than other devices in the spanning tree.

Example

```
awplus# configure terminal
awplus(config)# spanning-tree priority 4096
```

Related Commands spanning-tree mst instance priority

show spanning-tree

spanning-tree priority (port priority)

Overview Use this command in Interface Configuration mode for a switch port interface only to set the port priority for port. A lower priority value indicates a greater likelihood of the port becoming part of the active topology.

Use this command for RSTP, STP, or MSTP. When the device is in MSTP mode, this will apply to the CIST.

Use the **no** variant of this command to reset it to the default.

Syntax

```
spanning-tree priority <priority>
no spanning-tree priority
```

Parameter	Description
<priority>	<0-240>, in increments of 16. The port priority, which will be rounded down to a multiple of 16.

Default The default priority is 128.

Mode Interface Configuration mode for a switch port interface only.

Usage To force a port to be part of the active topology (for instance, become the root port or a designated port) use a lower value than other ports on the device. (This behavior is subject to network topology, and more significant factors, such as bridge ID.)

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree priority 16
```

Related Commands

spanning-tree mst instance priority

spanning-tree priority (bridge priority)

show spanning-tree

spanning-tree restricted-role

Overview Use this command in Interface Configuration mode for a switch port interface only to restrict the port from becoming a root port.

Use the **no** variant of this command to disable the restricted role functionality.

Syntax
```
spanning-tree restricted-role
no spanning-tree restricted-role
```

Default The restricted role is disabled.

Mode Interface Configuration mode for a switch port interface only.

Example
```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree restricted-role
```

spanning-tree restricted-tcn

Overview Use this command in Interface Configuration mode for a switch port interface only to prevent TCN (Topology Change Notification) BPDUs (Bridge Protocol Data Units) from being sent on a port. If this command is enabled, after a topology change a bridge is prevented from sending a TCN to its designated bridge.

Use the **no** variant of this command to disable the restricted TCN functionality.

Syntax

```
spanning-tree restricted-tcn
no spanning-tree restricted-tcn
```

Default The restricted TCN is disabled.

Mode Interface Configuration mode for a switch port interface only.

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# spanning-tree restricted-tcn
```

spanning-tree transmit-holdcount

Overview Use this command to set the maximum number of BPDU transmissions that are held back.

Use the **no** variant of this command to restore the default transmit hold-count value.

Syntax

```
spanning-tree transmit-holdcount
no spanning-tree transmit-holdcount
```

Default Transmit hold-count default is 3.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# spanning-tree transmit-holdcount
```

undebug mstp

Overview This command applies the functionality of the no debug mstp (RSTP and STP) command.

15 Link Aggregation Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure a static channel group (static aggregator) and dynamic channel group (LACP channel group, etherchannel or LACP aggregator). Link aggregation is also sometimes referred to as channeling.

NOTE: *AlliedWare Plus™ supports IEEE 802.3ad link aggregation and uses the Link Aggregation Control Protocol (LACP). LACP does not interoperate with devices that use Port Aggregation Protocol (PAgP).*

Link aggregation does not necessarily achieve exact load balancing across the links. The load sharing algorithm is designed to ensure that any given data flow always goes down the same link. It also aims to spread data flows across the links as evenly as possible.

Link aggregation hashes one or more of the source and destination MAC address, IP address and UDP/TCP ports to select a link on which to send a packet. So packet flow between a pair of hosts always takes the same link inside the Link Aggregation Group (LAG). The net effect is that the bandwidth for a given packet stream is restricted to the speed of one link in the LAG.

For example, for a 2 Gbps LAG that is a combination of two 1 Gbps ports, any one flow of traffic can only ever reach a maximum throughput of 1 Gbps. However, the hashing algorithm should spread the flows across the links so that when many flows are operating, the full 2 Gbps can be utilized.

For a description of static and dynamic link aggregation (LACP), and configuration examples, see the Link Aggregation Feature Overview and Configuration Guide.

Command List

channel-group

Overview Use this command to either create a new dynamic channel group while at the same time adding a port to it, or to add a port to an existing dynamic channel group. Note that you must also set the LACP mode to be either active or passive.

You can create up to 32 dynamic (LACP) channel groups (and up to 96 static channel groups).

Use the **no** variant of this command to turn off link aggregation on the device port. You will be returned to Global Configuration mode from Interface Configuration mode.

Syntax

```
channel-group <dynamic-channel-group-number> mode
{active|passive}
```

```
no channel-group
```

Parameter	Description
<dynamic-channel-group-number>	<1-32> Specify a dynamic channel group number for an LACP link. You can create up to 32 dynamic (LACP) channel groups (in addition to up to 96 static channel groups).
active	Enables initiation of LACP negotiation on a port. The port will transmit LACP dialogue messages whether or not it receives them from the partner device.
passive	Disables initiation of LACP negotiation on a port. The port will only transmit LACP dialogue messages if the partner device is transmitting them, i.e., the partner is in the active mode.

Mode Interface Configuration

Usage All the device ports in a channel-group must belong to the same VLANs, have the same tagging status, and can only be operated on as a group. All device ports within a channel group must have the same port speed and be in full duplex mode.

Once the LACP channel group has been created, it is treated as a device port, and can be referred to in most other commands that apply to device ports.

To refer to an LACP channel group in other LACP commands, use the channel group number. To specify an LACP channel group (LACP aggregator) in other commands, prefix the channel group number with **po**. For example, 'po2' refers to the LACP channel group with channel group number 2.

For more information about LACP, see the Link Aggregation Feature Overview and Configuration Guide which is available on our website at alliedtelesis.com.

Examples

To add device port1.0.6 to a newly created LACP channel group 2 use the commands below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# channel-group 2 mode active
```

To remove device port1.0.6 from any created LACP channel groups use the command below:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# no channel-group
```

To reference channel group 2 as an interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface po2
awplus(config-if)#
```

Related Commands

show etherchannel

show etherchannel detail

show etherchannel summary

show port etherchannel

clear lacp counters

Overview Use this command to clear all counters of all present LACP aggregators (channel groups) or a given LACP aggregator.

Syntax

```
clear lacp [<1-32>] counters
```

Parameter	Description
<1-32>	Channel-group number.

Mode Privileged Exec

Example

```
awplus# clear lacp 2 counters
```

debug lacp

Overview Use this command to enable all LACP troubleshooting functions.

Use the **no** variant of this command to disable this function.

Syntax

```
debug lacp {all|cli|event|ha|packet|sync|timer[detail]}
no debug lacp {all|cli|event|ha|packet|sync|timer[detail]}
```

Parameter	Description
`all`	Turn on all debugging for LACP.
`cli`	Specifies debugging for CLI messages. Echoes commands to the console.
`event`	Specifies debugging for LACP events. Echoes events to the console.
`ha`	Specifies debugging for HA (High Availability) events. Echoes High Availability events to the console.
`packet`	Specifies debugging for LACP packets. Echoes packet contents to the console.
`sync`	Specified debugging for LACP synchronization. Echoes synchronization to the console.
`timer`	Specifies debugging for LACP timer. Echoes timer expiry to the console.
`detail`	Optional parameter for LACP timer-detail. Echoes timer start/stop details to the console.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# debug lacp timer detail
awplus# debug lacp all
```

Related Commands show debugging lacp

undebug lacp

lacp global-passive-mode enable

Overview Use this command to enable LACP channel-groups to dynamically self-configure when they are connected to another device that has LACP channel-groups configured with Active Mode.

Syntax

```
lacp global-passive-mode enable
no lacp global-passive-mode enable
```

Default Enabled

Mode Global Configuration

Usage Do not mix LACP configurations (manual & dynamic). When LACP global passive mode is turned on (by using the **lacp global-passive-mode enable** command), we do not recommend using a mixed configuration in a LACP channel-group; i.e. some links are manually configured (by the **channel-group** command) and others are dynamically learned in the same channel-group.

Example To enable global passive mode for LACP channel groups, use the command:

```
awplus(config)# lacp global-passive-mode enable
```

To disable global passive mode for LACP channel groups, use the command:

```
awplus(config)# no lacp global-passive-mode enable
```

Related Commands show etherchannel

show etherchannel detail

lacp port-priority

Overview Use this command to set the priority of a device port. Ports are selected for aggregation based on their priority, with the higher priority (numerically lower) ports selected first.

Use the **no** variant of this command to reset the priority of port to the default.

Syntax

```
lacp port-priority <1-65535>
no lacp port-priority
```

Parameter	Description
<1-65535>	Specify the LACP port priority.

Default The default is 32768.

Mode Interface Configuration

Example

```
awplus# configure terminal
awplus(config)# interface port1.0.5
awplus(config-if)# lacp port-priority 34
```

lacp system-priority

Overview Use this command to set the system priority of a local system. This is used in determining the system responsible for resolving conflicts in the choice of aggregation groups.

Use the **no** variant of this command to reset the system priority of the local system to the default.

Syntax

```
lacp system-priority <1-65535>
no lacp system-priority
```

Parameter	Description
<1-65535>	LACP system priority. Lower numerical values have higher priorities.

Default The default is 32768.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# lacp system-priority 6700
```

lacp timeout

Overview Use this command to set the short or long timeout on a port. Ports will time out of the aggregation if three consecutive updates are lost.

Syntax

```
lacp timeout {short|long}
```

Parameter	Description
`timeout`	Number of seconds before invalidating a received LACP data unit (DU).
`short`	LACP short timeout. The **short** timeout value is **1** second.
`long`	LACP long timeout. The **long** timeout value is **30** seconds.

Default The default is **long** timeout (30 seconds).

Mode Interface Configuration

Usage This command enables the device to indicate the rate at which it expects to receive LACPDUs from its neighbor.

If the timeout is set to **long**, then the device expects to receive an update every **30** seconds, and this will time a port out of the aggregation if no updates are seen for 90 seconds (i.e. 3 consecutive updates are lost).

If the timeout is set to **short**, then the device expects to receive an update every second, and this will time a port a port out of the aggregation if no updates are seen for 3 seconds (i.e. 3 consecutive updates are lost).

The device indicates its preference by means of the Timeout field in the Actor section of its LACPDUs. If the Timeout field is set to 1, then the device has set the **short** timeout. If the Timeout field is set to 0, then the device has set the **long** timeout.

Setting the **short** timeout enables the device to be more responsive to communication failure on a link, and does not add too much processing overhead to the device (1 packet per second).

NOTE: *It is not possible to configure the rate that the device sends LACPDUs; the device must send at the rate which the neighbor indicates it expects to receive LACPDUs.*

Examples The following commands set the LACP long timeout period for 30 seconds on `port1.0.2`.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout long
```

The following commands set the LACP short timeout for 1 second on `port1.0.2`.

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# lacp timeout short
```

show debugging lacp

Overview Use this command to display the LACP debugging option set.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging lacp
```

Mode User Exec and Privileged Exec

Example

```
awplus# show debugging lacp
```

Output Figure 15-1: Example output from the **show debugging lacp** command

```
LACP debugging status:
 LACP timer debugging is on
 LACP timer-detail debugging is on
 LACP cli debugging is on
 LACP packet debugging is on
 LACP event debugging is on
 LACP sync debugging is on
```

Related Commands debug lacp

show diagnostic channel-group

Overview This command displays dynamic and static channel group interface status information. The output of this command is useful for Allied Telesis authorized service personnel for diagnostic purposes.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show diagnostic channel-group
```

Mode User Exec and Privileged Exec

Example
```
awplus# show diagnostic channel-group
```

Output Figure 15-2: Example output from the **show diagnostic channel-group** command

```
awplus#show diagnostic channel-group

Channel Group Info based on NSM:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503     port1.0.15   5015     No
     sa3        4503     port1.0.18   5018     No
     po1        4601     port1.0.7    5007     No
     po1        4601     port1.0.8    5008     No
     po1        4601     port1.0.9    5009     No


Channel Group Info based on HSL:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


Channel Group Info based on IPIFWD:
Note: Pos - position in hardware table
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a
```

```
Channel Group Info based on HW:
Note: Pos - position in hardware table
      Only entries from first device are displayed.
-------------------------------------------------------------
Dev  Interface  IfIndex  Member port  IfIndex  Active  Pos
-------------------------------------------------------------
     sa3        4503                           N/a
     po1        4601                           N/a


No error found
```

Related Commands show tech-support

show etherchannel

Overview Use this command to display information about a LACP channel specified by the channel group number.

The command output also shows the thrash limiting status. If thrash limiting is detected and the **thrash limiting** parameter of the thrash-limiting command is set to **vlan disable**, the output will also show the VLANs on which thrashing is detected.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show etherchannel [<1-32>]
```

Parameter	Description
<1-32>	Channel-group number.

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel 2
```

Output Example output from **show etherchannel** for a particular channel

```
% Lacp Aggregator: po1

 Thrash-limiting

 Status Vlan Thrashing Detected, Action vlan-disable 60(s)

 Thrashing Vlans 1 2 3 4 5
% Member:
   port1.0.4
   port1.0.6
```

show etherchannel detail

Overview Use this command to display detailed information about all LACP channels.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show etherchannel detail
```

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel detail
```

Output Example output from **show etherchannel detail**

```
awplus#show etherchannel detail
Aggregator po1 (IfIndex: 4601)
 Mac address: 00:00:cd:37:05:17
 Admin Key: 0001 - Oper Key 0001
 Receive link count: 2 - Transmit link count: 2
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,00-00-cd-37-02-9a,0x0001
  Link: port1.0.1 (IfIndex: 8002) synchronized
  Link: port1.0.2 (IfIndex: 20002) synchronized
Aggregator po2 (IfIndex: 4602)
 Mac address: 00:00:cd:37:05:17
 Admin Key: 0002 - Oper Key 0002
 Receive link count: 2 - Transmit link count: 2
 Individual: 0 - Ready: 1
 Partner LAG: 0x8000,ec-cd-6d-aa-c8-56,0x0002
  Link: port1.0.3 (IfIndex: 8001) synchronized
  Link: port1.0.4 (IfIndex: 20001) synchronized
```

show etherchannel summary

Overview Use this command to display a summary of all LACP channels.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show etherchannel summary
```

Mode User Exec and Privileged Exec

Example

```
awplus# show etherchannel summary
```

Output Example output from **show etherchannel summary**

```
awplus#show etherchannel summary
Aggregator po10 (IfIndex: 4610)
 Admin Key: 0010 - Oper Key 0010
  Link: port1.0.1 (IfIndex: 7007) synchronized
  Link: port1.0.2 (IfIndex: 8007) synchronized
  Link: port1.0.3 (IfIndex: 11007) synchronized
```

show lacp sys-id

Overview Use this command to display the LACP system ID and priority.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show lacp sys-id
```

Mode User Exec and Privileged Exec

Example

```
awplus# show lacp sys-id
```

Output Example output from **show lacp sys-id**

```
System Priority: 0x8000 (32768)
MAC Address: 0200.0034.5684
```

show lacp-counter

Overview Use this command to display the packet traffic on all ports of all present LACP aggregators, or a given LACP aggregator.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show lacp-counter [<1-32>]
```

Parameter	Description
<1-32>	Channel-group number.

Mode User Exec and Privileged Exec

Example

```
awplus# show lacp-counter 2
```

Output Example output from **show lacp-counter**

```
% Traffic statistics
Port          LACPDUs          Marker          Pckt err
           Sent     Recv     Sent     Recv     Sent     Recv
% Aggregator po2 (IfIndex: 4604)
port1.0.2   0        0        0        0        0        0
```

show port etherchannel

Overview Use this command to show LACP details of the device port specified.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show port etherchannel <port>
```

Parameter	Description
<port>	Name of the device port to display LACP information about.

Mode User Exec and Privileged Exec

Example

```
awplus# show port etherchannel port1.0.2
```

Output Example output from **show port etherchannel**

```
awplus#show port etherchannel port1.0.2
LACP link info: port1.0.2 - 7007
Link: port1.0.2 (IfIndex: 7007)
Aggregator: po10 (IfIndex: 4610)
Receive machine state: Current
Periodic Transmission machine state: Slow periodic
Mux machine state: Collecting/Distributing
Actor Information:                    Partner Information:
 Selected ................. Selected     Partner Sys Priority ....... 0x8000
 Physical Admin Key ..... 2             Partner System .. ec-cd-6d-d1-64-d0
 Port Key ..... 10                      Port Key ..... 10
 Port Priority ..... 32768              Port Priority ..... 32768
 Port Number ..... 7007                 Port Number ..... 5001
 Mode ..... Active                      Mode ..... Active
 Timeout ..... Long                     Timeout ..... Long
 Individual ..... Yes                   Individual ..... Yes
 Synchronised ..... Yes                 Synchronised ..... Yes
 Collecting ..... Yes                   Collecting ..... Yes
 Distributing ..... Yes                 Distributing ..... Yes
 Defaulted ..... No                     Defaulted ..... No
 Expired ..... No                       Expired ..... No
```

show static-channel-group

Overview Use this command to display all configured static channel groups and their corresponding member ports. Note that a static channel group is the same as a static aggregator.

The command output also shows the thrash limiting status. If thrash limiting is detected and the **thrash limiting** parameter of the thrash-limiting command is set to **vlan disable**, the output will also show the VLANs on which thrashing is detected.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide, which is available on our website at alliedtelesis.com.

Syntax

```
show static-channel-group
```

Mode User Exec and Privileged Exec

Example

```
awplus# show static-channel-group
```

Output Example output from **show static-channel-group**

```
% LAG Maximum        : 128
% LAG Static  Maximum: 96
% LAG Dynamic Maximum: 32
% LAG Static  Count  : 2
% LAG Dynamic Count  : 2
% LAG Total   Count  : 4
% Static Aggregator: sa2
% Member:
   port1.0.1
% Static Aggregator: sa3
% Member:
   port1.0.2
```

Related Commands static-channel-group

static-channel-group

Overview Use this command to create a static channel group, or add a member port to an existing static channel group. Static channel groups are also known as static aggregators.

You can create up to 96 static channel groups (and up to 32 dynamic channel groups).

Use the **no** variant of this command to remove the device port from the static channel group.

Syntax

```
static-channel-group <static-channel-group-number>
[member-filters]
```

```
no static-channel-group
```

Parameter	Description
<static-channel-group-number>	<1-96> Static channel group number.
member-filters	Allow QoS and ACL settings to be configured on the aggregator's individual member ports, instead of the aggregator itself. This configuration is required when using QoS Storm Protection on a static aggregator.

Mode Interface Configuration

Usage This command adds the device port to the static channel group with the specified channel group number. If the channel group does not exist, it is created, and the port is added to it. The **no** prefix detaches the port from the static channel group. If the port is the last member to be removed, the static channel group is deleted.

All the ports in a channel group must have the same VLAN configuration: they must belong to the same VLANs and have the same tagging status, and can only be operated on as a group.

Once the static channel group has been created, it is treated as a device port, and can be referred to in other commands that apply to device ports.

To refer to a static channel group in other static channel group commands, use the channel group number. To specify a static channel group in other commands, prefix the channel group number with **sa**. For example, 'sa2' refers to the static channel group with channel group number 2.

Examples To define static channel group 2 on a device port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# static-channel-group 2
```

To reference static channel group 2 as an interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)#
```

To make it possible to use QoS Storm Protection on static channel group 2 on port1.0.6, with an ACL named “test-acl”, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.6
awplus(config-if)# static-channel-group 2 member-filters
awplus(config-if)# access-group test-acl
```

Related Commands show static-channel-group

undebug lacp

Overview This command applies the functionality of the no debug lacp command.

16 Power over Ethernet Commands

Introduction

Overview This chapter contains an alphabetical list of commands used to configure Power over Ethernet (PoE). Each command contains a functional description and shows examples of configuration and output screens for show commands. These commands are only supported on PoE capable ports. An error message will display on the console if you enter a PoE command on a port that does not support PoE. The following documents offer further information for configuring PoE on AlliedWare Plus switches.

- the PoE Feature Overview and Configuration_Guide.
- the Support for Allied Telesis Enterprise_MIBs in AlliedWare Plus, for information about which PoE MIB objects are supported.
- the SNMP Feature Overview and Configuration_Guide, for information about SNMP traps.

Power over Ethernet (PoE) is a technology allowing devices such as IP phones to receive power over existing LAN cabling.

PoE is configured using the commands in this chapter. Note the Power Sourcing Equipment (PSE) referred to throughout this chapter is an Allied Telesis PoE switch running the AlliedWare Plus™ Operating System, supporting the IEEE 802.3af and IEEE 802.3at Power Ethernet standards. The Powered Device (PD) referred to throughout this chapter is a PoE or PoE+ powered device, such as an IP phone or a Wireless Access Point (WAP).

The commands in this chapter are available on the Allied Telesis IX5-28GPX switch. IX5-28GPX switches are Layer 2 PoE+ Gigabit Ethernet switches with SFP+ support.

NOTE: *Note that IX5-28GPX Layer 2 Gigabit Ethernet PoE+ switches with SFP / SFP+ support can have one or two hot-swappable AT-PWR800 (800 W) power supplies installed.*

*See the **IX5 Series Installation Guide** for information about PSU options.*

NOTE:

Command List

clear power-inline counters interface

Overview This command will clear the counters from a specified port, a range of ports, or all ports on the Power Sourcing Equipment (PSE). If no ports are entered then PoE counters for all ports are cleared. It will also clear all Power over Ethernet (PoE) counters supported by the Power Ethernet MIB (RFC 3621).

Syntax

```
clear power-inline counters interface [<port-list>]
```

Parameter	Description
<port-list>	Selects the port or ports whose counters are to be cleared.

Mode Privileged Exec

Usage The PoE counters are displayed with the show power-inline counters command.

Examples To clear the PoE counters for `port1.0.2`only, use the following command:

```
awplus# clear power-inline counters interface port1.0.2
```

To clear the PoE counters for `port1.0.1` through `port1.0.10`, use the following command:

```
awplus# clear power-inline counters interface
port1.0.1-port1.0.10
```

To clear the PoE counters for all ports, use the following command:

```
awplus# clear power-inline counters interface
```

Validation Commands show power-inline counters

debug power-inline

Overview This command enables debugging display for messages that are specific to Power over Ethernet (PoE).

Use the **no** variant of this command to disable the specified PoE debugging messages.

Syntax

```
debug power-inline [all|event|info|power]
no debug power-inline [all|event|info|power]
```

Parameter	Description
`all`	Displays all (`event`, `info`, `nsm`, `power`) debug messages.
`event`	Displays event debug information, showing any error conditions that may occur during PoE operation.
`info`	Displays informational level debug information, showing high-level essential debugging, such as information about message types.
`power`	Displays power management debug information.

Default No debug messages are enabled by default.

Mode Privileged Exec

Usage Use the terminal monitor command to display PoE debug messages on the console.

Use the show debugging power-inline command to show the PoE debug configuration.

Examples To enable PoE debugging and start the display of PoE `event` and `info` debug messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline event info
```

To enable PoE debugging and start the display of all PoE debugging messages on the console, use the following commands:

```
awplus# terminal monitor
awplus# debug power-inline all
```

To disable PoE debugging and stop the display of PoE `event` and `info` debug messages on the console, use the following command:

```
awplus# no debug power-inline event info
```

To disable all PoE debugging and stop the display of any PoE debugging messages on the console, use the following command:

```
awplus# no debug power-inline all
```

Validation Commands show debugging power-inline

Related Commands terminal monitor

power-inline allow-legacy

Overview This command enables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

The no variant of this command disables detection of pre-IEEE 802.3af Power Ethernet standard legacy Powered Devices (PDs).

Syntax

```
power-inline allow-legacy
no power-inline allow-legacy
```

Default Detection of legacy PDs is enabled on all ports on the Power Sourcing Equipment (PSE).

Mode Global Configuration

Examples To disable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline allow-legacy
```

To enable detection of legacy PDs, use the following commands:

```
awplus# configure terminal
awplus(config)# power-inline allow-legacy
```

Validation Commands show power-inline

show running-config power-inline

power-inline description

Overview This command adds a description for a Powered Device (PD) connected to a PoE port.

The **no** variant of this command clears a previously entered description for a connected PD, resetting the PD description to the default (null).

Syntax

```
power-inline description <pd-description>
no power-inline description
```

Parameter	Description
<pd-description>	Description of the PD connected to the PoE capable port (with a maximum 256 character string limit per PD description).

Default No description for a connected PD is set by default.

Mode Interface Configuration

Usage Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

Examples To add the description `Desk Phone` for a connected PD on `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline description Desk Phone
```

To clear the description as added above for the connected PD on `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline description
```

Validation Commands show power-inline interface

show running-config power-inline

power-inline enable

Overview This command enables Power over Ethernet (PoE) to detect a connected Powered Device (PD) and supply power from the Power Sourcing Equipment (PSE).

The **no** variant of this command disables PoE functionality on the selected PoE port(s). No power is supplied to a connected PD after PoE is disabled on the selected PoE port(s).

Syntax

```
power-inline enable
no power-inline enable
```

Default PoE is enabled by default on all ports on the PSE.

Mode Interface Configuration

Usage In a stack of IX5 switches this command is supported on all PoE capable ports.

Select a PoE port, a list of PoE ports, or a range of PoE ports from the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

No PoE log messages are generated for specified PoE port(s) after PoE is disabled. The disabled PoE port(s) still provide Ethernet connectivity after PoE is disabled.

Examples To disable PoE on ports `port1.0.1` to `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# no power-inline enable
```

To enable PoE on ports `port1.0.1` to `port1.0.4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# power-inline enable
```

Validation Commands

show power-inline

show power-inline interface

show power-inline interface detail

show running-config power-inline

power-inline max

Overview This command sets the "maximum" power allocated to a Power over an Ethernet (PoE and PoE+) port. The amount of power actually supplied to the port depends on the power requirements of the connected PD. It is also a function of the total PoE power loading on the switch and the PoE priority set for the port by the power-inline priority command. However this command (power-inline max) does apply a "maximum" value to the power that the port is able to supply.

Note that the value set by this command will be the figure the switch will use when apportioning the power budget for its ports. For example, if 15.4 W is assigned to a port whose PD only consumes 5 W, the switch will reserve the full 15.4 W for this port when determining its total power PoE power requirement.

The **no** variant of this command sets the maximum power supplied to a PoE port to the default, which is set to the maximum power limit for the class of the connected Powered Device (PD).

Syntax

```
power-inline max <4000-30000>
no power-inline max
```

Parameter	Description
<4000-30000>	The maximum power allocated to a PoE port in milliwatts (mW).

Default The Power Sourcing Equipment (PSE) supplies the maximum power limit for the class of the PD connected to the port by default.

NOTE: *See the PoE Feature Overview and Configuration Guide for further information about power classes.*

Mode Interface Configuration

Usage In a stack of IX5 switches this command is supported on all PoE capable ports.

Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

If you select a range of PoE ports in Interface Configuration mode before issuing this command, then each port in the range selected will have the same maximum power value configured. If the PoE port attempts to draw more than the maximum power, this is logged and all power is removed. Note that the value entered is rounded up to the next value supported by the hardware.

See the actual value used, as shown after command entry, in the sample console output below:

```
awplus#configure terminal

awplus(config)#interface
port1.0.1

awplus(config-if)#power-line max 5300

% The maximum power has been rounded to 5450mW in hardware.
```

See the LLDP Feature Overview and Configuration Guide for information about power monitoring at the PD.

Note the difference in power supplied from the PSE to the power available at the PD due to line loss.

See the PoE Feature Overview and Configuration Guide for further information about the difference between the power supplied from the PSE and the power available at the PD.

Examples To set the maximum power supplied to ports in the range `1.0.2 to 1.0.4` to 6450mW per port, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.4
awplus(config-if)# power-inline max 6450
```

To set the maximum power supplied to `port1.0.2`, to `6450` mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline max 6450
```

To clear the user-configured maximum power supplied to `port1.0.2`, and revert to using the default maximum power of 30000 mW, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline max
```

Validation Commands show power-inline interface

show running-config power-inline

power-inline priority

Overview This command sets the Power over Ethernet (PoE) priority level of a PoE port to one of three available priority levels:

- low
- high
- critical

The **no** variant of this command restores the PoE port priority to the default (low).

Syntax

```
power-inline priority {low|high|critical}
no power-inline priority
```

Parameter	Description
`low`	The lowest priority for a PoE enabled port (default). PoE ports set to `low` only receive power if all the PoE ports assigned to the other two levels are already receiving power.
`high`	The second highest priority for a PoE enabled port. PoE ports set to `high` receive power only if all the ports set to `critical` are already receiving power.
`critical`	The highest priority for a PoE enabled port. PoE ports set to `critical` are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all Critical ports are receiving power.

Default The default priority is `low` for all PoE ports on the Power Sourcing Equipment (PSE).

Mode Interface Configuration

Usage This command is supported on all PoE capable ports, whether operating as a stand-alone switch, or within a VCStack.

Select a PoE port, a list of PoE ports, or a range of PoE ports with the preceding interface (to configure) command. If you specify a range or list of ports they must all be PoE capable ports.

PoE ports with higher priorities are given power before PoE ports with lower priorities. If the priorities for two PoE ports are the same then the lower numbered PoE port is given power before the higher numbered PoE port.

See the PoE Feature Overview and Configuration Guide for further information about PoE priority.

Examples

To set the priority level to `high` for `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# power-inline priority high
```

To reset the priority level to the default for `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no power-inline priority
```

Validation Commands

show power-inline

show power-inline interface

show running-config power-inline

Related Commands

power-inline usage-threshold

power-inline usage-threshold

Overview This command sets the level at which the Power Sourcing Equipment (PSE) will issue a message that the power supplied to all Powered Devices (PDs) has reached a critical level of the nominal power rating for the PSE. The level is set as a percentage of total available power.

The **no** variant of this command resets the notification usage-threshold to the default (80% of the nominal power rating of the PSE).

Syntax

```
power-inline usage-threshold <1-99>
no power-inline usage-threshold
```

Parameter	Description
<1-99>	The usage-threshold percentage configured with this command.

Default The default power usage threshold is 80% of the nominal power rating of the PSE.

Mode Global Configuration

Usage Use the snmp-server enable trap command to configure SNMP notification. An SNMP notification is sent when the usage-threshold, as configured in the example, is exceeded.

Examples To generate SNMP notifications when power supplied exceeds 70% of the nominal PSE power, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
awplus(config)# power-inline usage-threshold 70
```

To reset the notification threshold to the default (80% of the nominal PSE power rating), use the following commands:

```
awplus# configure terminal
awplus(config)# no power-inline usage-threshold
```

Validation Commands show power-inline interface

show running-config power-inline

Related Commands snmp-server enable trap

service power-inline

Overview This command enables Power over Ethernet (PoE) globally on the Power Sourcing Equipment (PSE) for all PoE ports.

Syntax

```
service power-inline
no service power-inline
```

Default PoE functionality is enabled by default on the PSE.

Mode Global Configuration

Usage In a stack, issuing this command enables PoE globally for all PoE ports.

In a stack configuration, only stack members containing PoE hardware will have PoE enabled by default in software.

Examples To disable PoE on the PSE, use the following commands:

```
awplus# configure terminal
awplus(config)# no service power-inline
```

To re-enable PoE on the PSE, if PoE has been disabled, use the following commands:

```
awplus# configure terminal
awplus(config)# service power-inline
```

Validation Commands show power-inline

show running-config power-inline

show debugging power-inline

Overview This command displays Power over Ethernet (PoE) debug settings.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging power-inline
```

Mode User Exec and Privileged Exec

Example To display PoE debug settings, use the following command:

```
awplus# show debugging power-inline
```

Output Figure 16-1: Example output from the **show debugging power-inline** command

```
awplus#show debugging power-inline
PoE Debugging status:
PoE Informational debugging is disabled
PoE Event debugging is disabled
PoE Power Management debugging is disabled

PoE NSM debugging is enabled
```

Related Commands

debug power-inline

terminal monitor

show power-inline

Overview This command displays the Power over Ethernet (PoE) status for all ports on the Power Sourcing Equipment (PSE).

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show power-inline
```

Mode User Exec and Privileged Exec

Example To display the PoE status for all ports on the PSE, use the following command:

```
awplus# show power-inline
```

Output Figure 16-2: Example output from the **show power-inline** command

```
awplus#show power-inline
PoE Status:

Stack Member 2
 Nominal Power: 370W
 Power Allocated: 246W

 Actual Power Consumption: 151W
 Operational Status: On
 Power Usage Threshold: 80% (296W)

PoE Interface:
Interface  Admin   Pri  Oper    Power   Device    Class  Max(mW)
port2.0.1  Enabled Low  Powered  3840   n/a         1    4000 [C]
port2.0.2  Enabled High Powered  6720   n/a         2    7000 [C]
port2.0.3  Enabled Low  Powered 14784   n/a         3   15400 [C]
port2.0.4  Enabled Crit Powered 14784   n/a         3   15400 [C]
port2.0.5  Enabled Crit Powered  3840   n/a         1    4000 [C]
port2.0.6  Enabled High Powered  6720   n/a         2    7000 [C]
port2.0.7  Enabled Low  Powered 14784   n/a         3   15400 [C]
```

Table 1: Parameters in the **show power-inline** command output

Parameter	Description
`Nominal Power`	The nominal power available on the switch in watts (W).
`Power Allocated`	The current power allocated in watts (W) that is available to be drawn by any connected Powered Devices (PDs). This is updated every 5 seconds.

Table 1: Parameters in the **show power-inline** command output (cont.)

Parameter	Description
`Actual Power Consumption`	The current power consumption in watts (W) drawn by all connected Powered Devices (PDs). This is updated every 5 seconds.
`Operational Status`	The operational status of the PSU hardware on the PSE when this command was issued: • **On** if the PSU as installed inside the PSE is switched on. • **Off** when the PSU in the PSE is switched off (an RPS may be connected to the PSE to power PoE instead of the PSU). • **Fault** when there is an issue with the PSE PSU hardware.
`Power Usage Threshold (%)`	The configured SNMP trap / log threshold for the PSE, as configured from a power-inline usage-threshold command.
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`Admin`	The administrative state of PoE on a PoE port, either **Enabled** or **Disabled**.
`Pri`	The current PoE priorities for PoE ports on the PSE, as configured from a power-inline priority command: • **Low** displays when the `low` parameter is issued. The lowest priority for a PoE enabled port (default). • **High** displays when the `high` parameter is issued. The second highest priority for a PoE enabled port. • **Crit** displays when the `critical` parameter is issued. The highest priority for a PoE enabled port.
`Oper`	The current PSE PoE port state when this command was issued: • **Powered** displays when there is a PD connected and power is being supplied from the PSE. • **Disabled** displays when supplying power would make the PSE go over the power budget. • **Off** displays when PoE has been disabled for the PoE port. • **F ault** displays when a PSE goes over its power allocation.
`Power`	The power consumption in milliwatts (mW) for the PoE port when this command was entered.
`Device`	The description of the connected PD device if a description has been added with the power-inline description command. No description is shown for PDs not configured with the power-inline description command.

Table 1: Parameters in the **show power-inline** command output (cont.)

Parameter	Description
`Class`	The class of the connected PD, if power is being supplied to the PD from the PSE. See the **Power over Ethernet Introduction** chapter for further information about PD classes and the power levels assigned per class.
`Max (mW)`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: • **[U]** if the power limit for a port was user configured (with the power-inline max command). • **[L]** if the power limit for a port was supplied by LLDP. • **[C]** if the power limit for a port was supplied by the PD class.

Related Commands

show power-inline counters

show power-inline interface

show power-inline counters

Overview This command displays Power over Ethernet (PoE) event counters for ports on the Power Sourcing Equipment (PSE). The PoE event counters displayed can also be accessed by objects in the PoE MIB (RFC 3621). See the MIB Objects Feature Overview and Configuration Guide for information about which PoE MIB objects are supported.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show power-inline counters [<port-list>]
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display all PoE event counters for them.

Mode User Exec and Privileged Exec

Usage To display all PoE event counters for all PoE ports on the PSE, do not enter the optional interface parameter.

Examples To display all PoE event counters for all PoE ports on the PSE, use the command:

```
awplus# show power-inline counters
```

To display the PoE event counters for the port range `1.0.1` to `1.0.3`, use the command:

```
awplus# show power-inline counters interface port1.0.1-1.0.3
```

Output Figure 16-3: Example output from the **show power-inline counters** command

```
awplus#show power-inline counters interface port1.0.4-port1.0.12
PoE Counters:
Interface   MPSAbsent Overload Short Invalid Denied
port1.0.4   0         0        0     0       0
port1.0.5   0         0        0     0       0
port1.0.6   0         0        0     0       0
port1.0.7   0         0        0     0       0
port1.0.8   0         0        0     0       0
port1.0.9   0         0        0     0       0
port1.0.10  0         0        0     0       0
port1.0.11  0         0        0     0       0
port1.0.12  0         0        0     0       0
```

Table 2: Parameters in the **show power-inline counters** command output

Parameter	Description
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`MPSAbsent`	The number of instances when the PoE MPS (Maintain Power Signature) signal has been lost. The PoE MPS signal is lost when a PD is disconnected from the PSE. Also increments `pethPsePortMPSAbsentCounter` in the PoE MIB.
`Overload`	The number of instances when a PD exceeds its configured power limit (as configured by the power-inline max command). Also increments `pethPsePortOverLoadCounter` in the PoE MIB.
`Short`	The number of short circuits that have happened with a PD. Also increments `pethPsePortShortCounter` in the PoE MIB.
`Invalid`	The number of times a PD with an Invalid Signature (where the PD has an open or short circuit, or is a legacy PD) is detected. Also increments `pethPseInvalidSignatureCounter` in the PoE MIB.
`Denied`	The number of times a PD has been refused power due to power budget limitations for the PSE. Also increments `pethPsePortPowerDeniedCounter` in the PoE MIB.

Related Commands

clear power-inline counters interface

show power-inline

show power-inline interface

show power-inline interface

Overview This command displays a summary of Power over Ethernet (PoE) information for specified ports. If no ports are specified then PoE information is displayed for all ports on the Power Sourcing Equipment (PSE).

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show power-inline interface [<port-list>]
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display PoE specific information in the show output.

Mode User Exec and Privileged Exec

Usage To display PoE information for all PoE ports on the PSE, do not specify any ports.

Example To display the PoE port specific information for all PoE ports on the switch, use the following command:

```
awplus# show power-inline interface
```

To display the PoE port specific information for the port range `1.0.1` to `1.0.4`, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.4
```

Output Figure 16-4: Example output from the **show power-inline interface** command

```
awplus#show power-inline interface port1.0.1-port1.0.4
Interface  Admin    Pri  Oper     Power Device      Class Max(mW)
port1.0.1  Disabled Low  Disabled     0 n/a         n/a   n/a
port1.0.2  Enabled  High Powered   3840 Desk Phone  1     5000 [U]
port1.0.3  Enabled  Crit Powered   6720 AccessPoint 2     7000 [C]
port1.0.4  Disabled Low  Disabled     0 n/a         n/a   n/a
```

Table 3: Parameters in the **show power-inline interface** command output

Parameter	Description
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`Admin`	The administrative state of PoE on a PoE port, either **Enabled** or **Disabled**.

Table 3: Parameters in the **show power-inline interface** command output

Parameter	Description
`Pri`	The current PoE priorities for PoE ports on the PSE, as configured from a power-inline priority command: • **Low** displays when the `low` parameter is issued. The lowest priority for a PoE enabled port (default). • **High** displays when the `high` parameter is issued. The second highest priority for a PoE enabled port. • **Crit** displays when the `critical` parameter is issued. The highest priority for a PoE enabled port.
`Oper`	The current PSE PoE port state when this command was issued: • **Powered** displays when there is a PD connected and power is being supplied from the PSE. • **Denied** displays when supplying power would make the PSE go over the power budget. • **Disabled** displays when the PoE port is administratively disabled. • **Off** displays when PoE has been disabled for the port. • **Fault** displays when a PSE goes over its power allocation.
`Power`	The power consumption in milliwatts (mW) for the PoE port when this command was entered.
`Device`	The description of the connected PD device if a description has been added with the power-inline description command. No description is shown for PDs not configured with the power-inline description command.
`Class`	The class of the connected PD, if power is being supplied to the PD from the PSE. See the PoE Feature Overview and Configuration Guide for further information about power classes.
`Max (mW)`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: • **[U]** if the power limit for a port was user configured (with the **power-inline max** command). • **[L]** if the power limit for a port was supplied by LLDP. • **[C]** if the power limit for a port was supplied by the PD class.

Related Commands

show power-inline

show power-inline interface detail

show power-inline interface detail

Overview This command displays detailed information for specified Power over Ethernet (PoE) port(s) on the Power Sourcing Equipment (PSE).

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show power-inline interface [<port-list>] detail
```

Parameter	Description
<port-list>	Enter the PoE port(s) to display the PoE port specific information.

Mode User Exec and Privileged Exec

Usage To show detailed PoE information for all ports on the PSE, do not specify any ports.

The power allocated to each port is listed in the `Power allocated` row, and is limited by the maximum power per Powered Device (PD) class, or a user configured power limit.

Example To display detailed PoE port specific information for the port range `1.0.1` to `1.0.2`, use the following command:

```
awplus# show power-inline interface port1.0.1-port1.0.2 detail
```

Output Figure 16-5: Example output from the **show power-inline interface detail** command

```
awplus#show power-inline interface port1.0.1-1.0.2 detail
Interface port1.0.1
  Powered device type: Desk Phone #1
  PoE admin enabled
  Priority Low
  Detection status: Powered
  Current power consumption: 4800 mW
  Powered device class: 1
  Power allocated: 5000 mW (from configuration)
  Detection of legacy devices is disabled
  Powered pairs: Data
Interface port1.0.2
  Powered device type: Access Point #3
  PoE admin enabled
  Priority High
  Detection status: Powered
  Current power consumption: 6720 mW
  Powered device class: 2
  Power allocated: 7000 mW (from powered device class)
  Detection of legacy devices is enabled
  Powered pairs: Data
```

Table 4: Parameters in **show power-inline interface detail** command output

Parameter	Description
`Interface`	The PoE port(s) in the format `portx.y.z`, where `x` is the device number, `y` is the module number within the device, and `z` is the PoE port number within the module.
`Powered device type:`	The name of the PD, if connected and if power is being supplied to the PD from the PSE, configured with the power-inline description command. **n/a** displays if a description has not been configured for the PD.
`PoE admin`	The administrative state of PoE on a PoE capable port, either **Enabled** or **Disabled** as configured from the power-inline enable command or the **no power-inline enable** command respectively.
`Priority`	The PoE priority of a port, which is either **Low,** or **High,** or **Critical**, as configured by the power-inline priority command.

Table 4: Parameters in **show power-inline interface detail** command output

Parameter	Description
`Detection status:`	The current PSE PoE port state when this command was issued: • **Powered** displays when there is a PD connected and power is being supplied from the PSE. • **Denied** displays when supplying power would make the PSE go over the power budget. • **Disabled** displays when the PoE port is administratively disabled. • **Off** displays when PoE has been disabled for the port. • **Fault** displays when a PSE goes over its power allocation.
`Current power consumption:`	The power consumption for the PoE port when this command was entered. Note that the power consumption may have changed since the command was entered and the power is displayed.
`Powered device class:`	The class of the connected PD if connected, and if power is being supplied to the PD from the PSE. See the PoE Feature Overview and Configuration Guide for further information about power classes.
`Power allocated:`	The power in milliwatts (mW) allocated for the PoE port. Additionally, note the following as displayed per PoE port: • **[U]** if the power limit for a port was user configured (with the **power-inline max** command). • **[L]** if the power limit for a port was supplied by LLDP. • **[C]** if the power limit for a port was supplied by the PD class.
`Detection of legacy devices is`	`[Enabled|Disabled]` The status of legacy PoE detection on the PoE port, as configured for the PoE port with the power-inline allow-legacy command.
`Powered pairs:`	`[Data|Spare]` The IEEE 802.3af and IEEE 802.3at standards allow for either **data** or **spare** twisted pairs to be used to transfer power to a PD. The powered pairs status for each port. AlliedWare Plus™ PoE switches implement IEEE 802.3af and IEEE 802.3at Endpoint PSE Alternative A (**Data**).

Related Commands

show power-inline

show power-inline interface

17 GVRP Commands

Introduction

Overview

With GVRP enabled the switch can exchange VLAN configuration information with other GVRP enabled switches. VLANs can be dynamically created and managed through trunk ports.

- There is limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.
- MSTP is not supported by the AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.
- VCStack is not supported by the current AlliedWare Plus GVRP implementation.

This chapter provides an alphabetical reference for commands used to configure GVRP. For information about GVRP, including configuration, see the GVRP Feature Overview and Configuration Guide.

Command List

- "show gvrp timer" on page 663

clear gvrp statistics

Overview Use this command to clear the GVRP statistics for all switchports, or for a specific switchport.

Syntax

```
clear gvrp statistics {all|<interface>}
```

Parameter	Description
`all`	Specify all switchports to clear GVRP statistics.
`<interface>`	Specify the switchport to clear GVRP statistics.

Mode Privileged Exec

Usage Use this command together with the show gvrp statistics command to troubleshoot GVRP.

Examples To clear all GVRP statistics for all switchport on the switch, enter the command:

```
awplus# clear gvrp statistics all
```

To clear GVRP statistics for switchport interface `port1.0.3`, enter the command:

```
awplus# clear gvrp statistics port1.0.3
```

Related Commands show gvrp statistics

debug gvrp

Overview Use this command to debug GVRP packets and commands, sending output to the console.

Use the **no** variant of this command to turn off debugging for GVRP packets and commands.

Syntax

```
debug gvrp {all|cli|event|packet}
no debug gvrp {all|cli|event|packet}
```

Parameter	Description
`all`	Specifies debugging for all levels.
`cli`	Specifies debugging for commands.
event	Specified debugging for events.
`packet`	Specifies debugging for packets.

Mode Privileged Exec and Global Configuration

Examples To enable GVRP on interfaces `port1.0.1-port1.0.2`, enter the commands:

```
awplus# configure terminal
awplus(config)# gvrp enable
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# gvrp
```

To disable GVRP on interfaces `port1.0.1-port1.0.2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# no gvrp
```

Examples To send debug output to the console for GVRP packets and GVRP commands, and to enable the display of debug output on the console first, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp all
```

To send debug output for GVRP packets to the console, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp packets
```

To send debug output for GVRP commands to the console, enter the commands:

```
awplus# terminal monitor
awplus# configure terminal
awplus(config)# debug gvrp cli
```

To stop sending debug output for GVRP packets and GVRP commands to the console, and to stop the display of any debug output on the console, enter the commands:

```
awplus# terminal no monitor
awplus# configure terminal
awplus(config)# no debug gvrp all
```

Related Commands

show debugging gvrp

terminal monitor

gvrp (interface)

Overview Use this command to enable GVRP for switchport interfaces.

Use the **no** variant of this command to disable GVRP for switchport interfaces.

Syntax

```
gvrp
no gvrp
```

Mode Interface Configuration (for switchport interfaces).

Default Disabled by default.

Usage Use this command to enable GVRP on switchport interfaces. Note this command does not enable GVRP for the switch. To enable GVRP on switchports use this command in Interface Configuration mode. You must issue a gvrp enable (global) command before issuing a gvrp (interface) command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

NOTE: *MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.*

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

Examples To enable GVRP on interfaces `port1.0.1-port1.0.2`, enter the commands:

```
awplus# configure terminal
awplus(config)# gvrp enable
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# gvrp
```

To disable GVRP on interfaces `port1.0.1-port1.0.2`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# no gvrp
```

Validation Commands show gvrp configuration

Related Commands gvrp dynamic-vlan-creation

gvrp enable (global)

gvrp dynamic-vlan-creation

Overview Use this command to enable dynamic VLAN creation globally for the switch.

Use the **no** variant of this command to disable dynamic VLAN creation globally for the switch.

Syntax

```
gvrp dynamic-vlan-creation
no gvrp dynamic-vlan-creation
```

Mode Global Configuration

Default Disabled by default.

Usage You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

You must also enable GVRP globally in Global Configuration mode before enabling GVRP on an interface in Interface Configuration mode. Both of these tasks must occur to create VLANs.

NOTE: *There is limit of 400 VLANs supported by the AlliedWare Plus GVRP implementation. VLANs may be numbered 1-4094, but a limit of 400 of these VLANs are supported.*

Examples Enter the following commands for switches with hostnames `switch1` and `switch2` respectively, so `switch1` propagates VLANs to `switch2` and `switch2` propagates VLANs to `switch1`:

Switch1:

```
switch1# configure terminal
switch1(config)# gvrp enable
switch1(config)# gvrp dynamic-vlan-creation
```

Switch2:

```
switch2# configure terminal
switch2(config)# gvrp enable
switch2(config)# gvrp dynamic-vlan-creation
```

To disable GVRP dynamic VLAN creation on the switch, enter the commands:

```
awplus# configure terminal
awplus(config)# no gvrp dynamic-vlan-creation
```

Validation Commands show gvrp configuration

Related Commands gvrp enable (global)

gvrp enable (global)

Overview Use this command to enable GVRP globally for the switch.

Use the **no** variant of this command to disable GVRP globally for the switch.

Syntax

```
gvrp enable
no gvrp enable
```

Mode Global Configuration

Default Disabled by default.

Usage Use this command to enable GVRP on the switch. Note that this command does not enable GVRP on switchports. To enable GVRP on switchports use the gvrp (interface) command in Interface Configuration mode. You must issue a gvrp enable (global) command before issuing a gvrp (interface) command.

You must enable GVRP on both ends of a link for GVRP to propagate VLANs between links.

NOTE: *MSTP is not supported by the current AlliedWare Plus GVRP implementation. GVRP and MSTP are mutually exclusive. STP and RSTP are supported by GVRP.*

Private VLAN trunk ports are not supported by the current AlliedWare Plus GVRP implementation. GVRP and private VLAN trunk ports are mutually exclusive.

Examples To enable GVRP for the switch, before enabling GVRP on switchports, enter the commands:

```
awplus# configure terminal
awplus(config)# gvrp enable
```

To disable GVRP on the switch, which will also disable GVRP enabled on switchports, enter the commands:

```
awplus# configure terminal
awplus(config)# no gvrp enable
```

Validation Commands show gvrp configuration

Related Commands gvrp (interface)

gvrp dynamic-vlan-creation

gvrp registration

Overview Use this command to set GVRP registration to normal, fixed, and forbidden registration modes.

Use the **no** variant of this command to disable GVRP registration.

Syntax

```
gvrp registration {normal|fixed|forbidden}
no gvrp registration {normal|fixed|forbidden}
```

Parameter	Description
`normal`	Specify dynamic GVRP registration and deregistration of VLANs.
`fixed`	Specify fixed GVRP registration and deregistration of VLANs.
`forbidden`	Specify no GVRP registration of VLANs. VLANs are deregistered.

Mode Interface Configuration

Default Normal registration is the default.

Usage Configuring a trunk port in normal registration mode allows dynamic creation of VLANs. Normal mode is the default mode. Validate using the show gvrp configuration command.

Configuring a trunk port in fixed registration mode allows manual creation of VLANs.

Configuring a trunk port in forbidden registration mode prevents VLAN creation on the port.

Examples To configure GVRP registration to `fixed` on `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# gvrp registration fixed
```

To disable GVRP registration on interfaces `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no gvrp registration
```

Validation Commands show gvrp configuration

gvrp timer

Overview Use this command to set GVRP timers in Interface Configuration mode for a given interface.

Use the **no** variant of this command to reset the GVRP timers to the defaults specified in the table below.

Syntax

```
gvrp timer {join <timer-value>|leave <timer-value>|leaveall
<timer-value>}
no gvrp timer {join|leave|leaveall}
```

Parameter	Description
`join`	Specifies the timer for joining the group (default is 20 centiseconds / hundredths of a second, or 200 milliseconds).
`leave`	Specifies the timer for leaving a group (default is 60 centiseconds / hundredths of a second, or 600 milliseconds).
`leaveall`	Specifies the timer for leaving all groups (default is 1000 centiseconds / hundredths of a second, or 10,000 milliseconds).
<timer-value>	<1-65535> The timer value in hundredths of a second (centiseconds).

Mode Interface Configuration

Defaults The default join time value is 20 centiseconds (200 milliseconds), the default leave timer value is 60 centiseconds (600 milliseconds), and the default leaveall timer value is 1000 centiseconds (10,000 milliseconds).

Usage When configuring the `leave` timer, set it to more than or equal to three times the `join` timer value. The settings for the `leave` and `join` timers must be the same for all GVRP enabled switches. See also the section "Setting the GVRP Timers" in the GVRP Feature Overview and Configuration Guide.

Use the show gvrp timer command to confirm GVRP timers set with this command.

Examples To set the GVRP `join` timer to 30 hundredths of a second (300 milliseconds) for interface `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# gvrp timer join 30
```

To set the GVRP `leave` timer to 90 hundredths of a second (900 milliseconds) for interface `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# gvrp timer leave 90
```

To reset the GVRP `join` timer to its default of 20 hundredths of a second for interface `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no gvrp timer join
```

Related Commands show gvrp timer

show debugging gvrp

Overview Use this command to display the GVRP debugging option set.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging gvrp
```

Mode User Exec and Privileged Exec

Example Enter the following commands to display GVRP debugging output on the console:

```
awplus# configure terminal
awplus(config)# debug gvrp all
awplus(config)# exit
awplus# show debugging gvrp
```

Output See sample output from the **show debugging gvrp** command after entering **debug gvrp all**:

```
GVRP debugging status:
  GVRP Event debugging is on
  GVRP CLI debugging is on
  GVRP Timer debugging is on
  GVRP Packet debugging is on
```

Related Commands debug gvrp

show gvrp configuration

Overview Use this command to display GVRP configuration data for a switch.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show gvrp configuration
```

Mode User Exec and Privileged Exec

Example To show GVRP configuration for the switch, enter the command:

```
awplus# show gvrp configuration
```

Output The following is an output of this command displaying the GVRP configuration for a switch:

```
awplus#show gvrp configuration
Global GVRP Configuration:
GVRP Feature: Enabled
Dynamic Vlan Creation: Disabled
Port based GVRP Configuration:
                                          Timers(centiseconds)
Port    GVRP Status Registration  Applicant   Join   Leave LeaveAll
---------------------------------------------------------------
port1.0.1 Enabled   Normal        Normal      20      60    1000
port1.0.2 Enabled   Normal        Normal      200    600   10000
```

show gvrp machine

Overview Use this command to display the state machine for GVRP.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show gvrp machine
```

Mode User Exec and Privileged Exec

Example To show the GVRP state machine for the switch, enter the command:

```
awplus# show gvrp machine
```

Output See the following output of this command displaying the GVRP state machine.

```
awplus  show gvrp machine
  port = 1.0.1  applicant state = QA   registrar state = INN
  port = 1.0.2  applicant state = QA   registrar state = INN
```

show gvrp statistics

Overview Use this command to display a statistical summary of GVRP information for the switch.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show gvrp statistics [<interface>]
```

Parameter	Description
<interface>	The name of the switchport interface.

Mode User Exec and Privileged Exec

Usage Use this command together with the clear gvrp statistics command to troubleshoot GVRP.

Examples To show the GVRP statistics for all switchport interfaces, enter the command:

```
awplus# show gvrp statistics
```

To show the GVRP statistics for switchport interfaces `port1.0.1` and `port1.0.2`, enter the command:

```
awplus# show gvrp statistics port1.0.1-port1.0.2
```

Output The following is an output of this command displaying a statistical summary for `port1.0.1-port1.0.2`

```
awplus#  show gvrp statistics port1.0.1-port1.0.2
Port     JoinEmpty    JoinIn   LeaveEmpty     LeaveIn      Empty
-------------------------------------------------------------------
1.0.1    RX           0          2          0         0        0
         TX           0          0          0         0        0
1.0.2    RX           0          1          0         0        1
         TX           0          0          0         0        0
```

Related Commands clear gvrp statistics

show gvrp timer

Overview Use this command to display data for the GVRP timers set with the gvrp timer command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show gvrp timer <interface>
```

Parameter	Description
<interface>	The name of the switchport interface.

Mode User Exec and Privileged Exec

Examples To show the GVRP timers for all switchport interfaces, enter the command:

```
awplus# show gvrp timer
```

To show the GVRP timers for switchport interface `port1.0.1`, enter the command:

```
awplus# show gvrp timer port1.0.1
```

Output The following show output displays data for timers on the switchport interface `port1.0.1`

```
awplus#  show gvrp timer port1.0.1
Timer           Timer Value (centiseconds)
----------------------------------------
Join                20
Leave               60
Leave All           1000
```

Related Commands gvrp timer

Part 3: Layer Three, Switching and Routing

18 IP Addressing and Protocol Commands

Introduction

Overview

This chapter provides an alphabetical reference of commands used to configure various IP features, including the following protocols:

- Address Resolution Protocol (ARP)
- Domain Name Service (DNS)

For more information, see the IP Feature Overview and Configuration Guide.

Command List

arp-aging-timeout

Overview This command sets a timeout period on dynamic ARP entries associated with a specific interface. If your device stops receiving traffic for the host specified in a dynamic ARP entry, it deletes the ARP entry from the ARP cache after this timeout is reached.

Your device times out dynamic ARP entries to ensure that the cache does not fill with entries for hosts that are no longer active. Static ARP entries are not aged or automatically deleted.

By default the time limit for dynamic ARP entries is 300 seconds on all interfaces.

The **no** variant of this command sets the time limit to the default of 300 seconds.

Syntax

```
arp-aging-timeout <0-432000>
no arp-aging timeout
```

Parameter	Description
<0-432000>	The timeout period in seconds.

Default 300 seconds (5 minutes)

Mode Interface Configuration for a VLAN interface.

Example To set the ARP entries on interface `vlan30` to time out after two minutes, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan30
awplus(config-if)# arp-aging-timeout 120
```

Related Commands

clear arp-cache

show arp

arp-mac-disparity

Overview Use this command to enable the switch to support services like Microsoft Network Load Balancing (MS-NLB).

Such services use ARP with disparate MAC addresses to ensure that packets destined for a server cluster virtual address are sent to all servers in the cluster. Disparate MAC addresses mean that the MAC address in the "sender hardware address" field of an ARP reply is different to the MAC address in the "Source MAC address" field of the Ethernet header that the ARP packet is encapsulated in.

The **no** variant of this command reverts to the default behavior. See the Default section below for more information.

Syntax

```
arp-mac-disparity {multicast|multicast-igmp|unicast}
no arp-mac-disparity {multicast|multicast-igmp|unicast}
```

Parameter	Description
`multicast`	Enables support of server clusters operating in multicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.
`multicast-igmp`	Enables support of server clusters operating in multicast/IGMP mode. In multicast/IGMP mode, the MS-NLB server cluster uses IGMP reports to forward server traffic to a limited set of ports.
`unicast`	Enables support of server clusters operating in unicast mode. Packets destined for the server cluster are flooded to all ports in the VLAN.

Default ARP-MAC disparity support is disabled and:

- If the disparate ARP has a multicast MAC address in the ARP reply, the switch drops the ARP reply and does not learn any associated addresses
- If the disparate ARP has a unicast MAC address in the ARP reply, the switch learns the address in the ARP reply. The learned ARP entry points to the single port that the ARP reply arrived on. Matching traffic will go out this port.

Mode Interface Configuration for a VLAN interface.

Usage When you are using **multicast** mode, you can limit the number of ports that packets are flooded to, instead of flooding to all ports in the VLAN. To do this, specify the list of ports when creating the ARP entry.

For example, to flood only port1.0.1 to port1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp 10.10.1.100 010e.11ff.2222
port1.0.1-port1.0.3
```

Examples To enable support for MS-NLB in unicast mode on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-mac-disparity unicast
```

To disable support for MS-NLB in unicast mode on interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no arp-mac-disparity unicast
```

Related Commands

arp (IP address MAC)

clear arp-cache

show arp

arp (IP address MAC)

Overview This command adds a static ARP entry to the ARP cache. This is typically used to add entries for hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist. Use the **alias** parameter to allow your device to respond to ARP requests for this IP address.

The **no** variant of this command removes the static ARP entry. Use the clear arp-cache command to remove the dynamic ARP entries in the ARP cache.

Syntax

```
arp <ip-addr> <mac-address> [<port-number>] [alias]
no arp <ip-addr>
```

Parameter	Description
<ip-addr>	The IPv4 address of the device you are adding as a static ARP entry.
<mac-address>	The MAC address of the device you are adding as a static ARP entry, in hexadecimal notation with the format HHHH.HHHH.HHHH.
<port-number>	The port number associated with the IP address. Specify this when the IP address is part of a VLAN.
alias	Allows your device to respond to ARP requests for the IP address. Proxy ARP must be enabled on the interface before using this parameter.

Mode Global Configuration

Examples To add the IP address 10.10.10.9 with the MAC address 0010.2533.4655 into the ARP cache, and have your device respond to ARP requests for this address, use the commands:

```
awplus# configure terminal
awplus(config)# arp 10.10.10.9 0010.2355.4566 alias
```

Related Commands

arp-mac-disparity

clear arp-cache

ip proxy-arp

show arp

arp log

Overview This command enables the logging of dynamic and static ARP entries in the ARP cache. The ARP cache contains mappings of device ports, VLAN IDs, and IP addresses to physical MAC addresses for hosts.

This command can display the MAC addresses in the ARP log either using the default hexadecimal notation (HHHH.HHHH.HHHH), or using the IEEE standard hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command to disable the logging of dynamic and static ARP entries in the ARP cache.

Syntax

```
arp log [mac-address-format ieee]
no arp log [mac-address-format ieee]
```

Parameter	Description
`mac-address-format ieee`	Display the MAC address in hexadecimal notation with the standard IEEE format (HH-HH-HH-HH-HH-HH), instead of displaying the MAC address with the default hexadecimal format (HHHH.HHHH.HHHH).

Default The ARP logging feature is disabled by default.

Mode Global Configuration

Usage You have the option to change how the MAC address is displayed in the ARP log message, to use the default hexadecimal notation (HHHH.HHHH.HHHH), or the IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH) when you apply the **mac-address-format ieee** parameter.

Enter the **arp log** command without the optional **mac-address-format ieee** parameter specified for MAC addresses in the ARP log output to use the default hexadecimal notation (HHHH.HHHH.HHHH).

Enter the **arp log mac-address-format ieee** command for MAC addresses in the ARP log output to use the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH).

Use the **no** variant of this command (**no arp log**) without the optional **mac-address- format ieee** parameter specified to disable ARP logging on the device

Use the **no** variant of this command with the optional **mac-address-format ieee** parameter specified (**no arp log mac-address-format ieee**) to disable IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) and revert to the default hexadecimal notation (HHHH.HHHH.HHHH) for MAC addresses in the ARP log output.

To display ARP log messages use the **show log | include ARP_LOG** command.

Examples To enable ARP logging and use the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

```
awplus# configure terminal
awplus(config)# arp log
```

To disable ARP logging on the device of MAC addresses displayed using the default hexadecimal notation (HHHH.HHHH.HHHH), use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log
```

To enable ARP logging and to specify that the MAC address in the log message is displayed in the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), use the following commands:

```
awplus# configure terminal
awplus(config)# arp log mac-address-format ieee
```

To disable ARP logging on the device of MAC addresses displayed using the standard IEEE format hexadecimal notation (HH-HH-HH-HH-HH-HH), and revert to the use of the default hexadecimal notation (HHHH.HHHH.HHHH) instead, use the following commands:

```
awplus# configure terminal
awplus(config)# no arp log mac-address-format ieee
```

To display ARP log messages, use following command:

```
awplus# show log | include ARP_LOG
```

Output Below is example output from the **show log | include ARP_LOG** command after enabling ARP logging displaying default hexadecimal notation MAC addresses (HHHH.HHHH.HHHH) using the **arp log** command.

```
awplus#configure terminal
awplus(config)#arp log
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr  6 06:21:01 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add
0013.4078.3b98 (192.168.2.4)
2010 Apr  6 06:22:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del
0013.4078.3b98 (192.168.2.4)
2010 Apr  6 06:23:26 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add
0030.940e.136b (192.168.2.20)
2010 Apr  6 06:23:30 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below is example output from the **show log | include ARP_LOG** command after enabling ARP logging displaying IEEE standard format hexadecimal notation MAC addresses (HH- HH-HH-HH-HH-HH) using the **arp log mac-address format ieee** command.

Table 1: Example output from the **show log | include ARP_LOG** command

```
awplus#configure terminal
awplus(config)#arp log mac-address-format ieee
awplus(config)#exit
awplus#show log | include ARP_LOG
2010 Apr  6 06:25:28 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-
17-9a-b6-03-69 (192.168.2.12)
2010 Apr  6 06:25:30 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 add 00-
03-37-6b-a6-a5 (192.168.2.10)
2010 Apr  6 06:26:53 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-
30-94-0e-13-6b (192.168.2.20)
2010 Apr  6 06:27:31 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-
17-9a-b6-03-69 (192.168.2.12)
2010 Apr  6 06:28:09 user.notice awplus HSL[1007]: ARP_LOG port1.0.6 vlan1 del 00-
03-37-6b-a6-a5 (192.168.2.10)
2010 Apr  6 06:28:14 user.notice awplus IMISH[1830]: show log | include ARP_LOG
```

Below are the parameters in output of the **show log | include ARP_LOG** command with an ARP log message format of <ARP_LOG> <port number> <VLAN ID> <Operation> <MAC> <IP> after <*date*> <*time*> <*severity*> <*hostname*> <*program-name*> information.

Table 2: Parameters in output of the **show log | include ARP_LOG** command

Parameter	Description
<ARP_LOG>	Indicates ARP log entry information follows <*date*> <*time*> <*severity*> <*hostname*> <*program name*> log information.
<port number>	Indicates device port number for the ARP log entry.
<VLAN ID>	Indicates the VLAN ID for the ARP log entry.
<Operation>	Indicates 'add' if the ARP log entry displays an ARP addition. Indicates 'del' if the ARP log entry displays an ARP deletion.
<MAC>	Indicates the MAC address for the ARP log entry, either in the default hexadecimal notation (HHHH.HHHH.HHHH) or in the IEEE standard format hexadecimal notation (HH-HH-HH-HH-HH-HH) as specified with the **arp log** or the **arp log mac-address-format ieee** command.
<IP>	Indicates the IP address for the ARP log entry.

Validation Commands show running-config

Related Commands show log

arp opportunistic-nd

Overview This command changes the behavior for unsolicited ARP packet forwarding on the device.

Use this command to enable opportunistic neighbor discovery for the global ARP cache.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global ARP cache.

Syntax

```
arp opportunistic-nd
no arp opportunistic-nd
```

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ARP packets (but not gratuitous ARP packets). The source MAC address for the unsolicited ARP packet is added to the ARP cache, so the device forwards the ARP packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ARP packet is not added to the ARP cache, so the ARP packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# arp opportunistic-nd
```

To disable opportunistic neighbor discovery for the global ARP cache, enter:

```
awplus# configure terminal
awplus(config)# no arp opportunistic-nd
```

Related Commands ipv6 opportunistic-nd

show arp

Validation Commands show running-config interface

arp-reply-bc-dmac

Overview Use this command to allow processing of ARP replies that arrive with a broadcast destination MAC (ffff.ffff.ffff). This makes neighbors reachable if they send ARP responses that contain a broadcast destination MAC.

Use the **no** variant of this command to turn off processing of ARP replies that arrive with a broadcast destination MAC.

Syntax

```
arp-reply-bc-dmac
no arp-reply-bc-dmac
```

Default By default, this functionality is disabled.

Mode Interface Configuration for VLAN interfaces

Example To allow processing of ARP replies that arrive on VLAN2 with a broadcast destination MAC, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# arp-reply-bc-dmac
```

Related Commands clear arp-cache

show arp

clear arp-cache

Overview This command deletes dynamic ARP entries from the ARP cache. You can optionally specify the IPv4 address of an ARP entry to be cleared from the ARP cache.

Syntax

```
clear arp-cache [<ip-address>]
```

Parameter	Description
<ip-address>	The IPv4 address of an ARP entry that is to be cleared from the ARP cache.

Mode Privileged Exec

Usage To display the entries in the ARP cache, use the show arp command. To remove static ARP entries, use the no variant of the arp (IP address MAC) command.

Example To clear all dynamic ARP entries, use the command:

```
awplus# clear arp-cache
```

To clear all dynamic ARP entries associated with the IPv4 address 192.168.1.1, use the command:

```
awplus# clear arp-cache 192.168.1.1
```

Related Commands

arp-mac-disparity

arp (IP address MAC)

show arp

clear ip dns forwarding cache

Overview Use this command to clear the DNS Relay name resolver cache.

Syntax

```
clear ip dns forwarding cache
```

Mode Privileged Exec

Examples To clear all cached data, use the command:

```
awplus# clear ip dns forwarding cache
```

Related Commands ip dns forwarding cache

debug ip dns forwarding

Overview Use this command to enable DNS Relay debugging.

Use the **no** variant of this command to disable DNS Relay debugging.

Syntax

```
debug ip dns forwarding
no debug ip dns forwarding
```

Default DNS Relay debugging is disabled by default.

Mode Privileged Exec

Examples To enable DNS forwarding debugging, use the commands:

```
awplus# debug ip dns forwarding
```

To disable DNS forwarding debugging, use the commands:

```
awplus# no debug ip dns forwarding
```

Related Commands ip dns forwarding

show debugging ip dns forwarding

debug ip packet interface

Overview The **debug ip packet interface** command enables IP packet debug and is controlled by the **terminal monitor** command.

If the optional **icmp** keyword is specified then ICMP packets are shown in the output.

The **no** variant of this command disables the **debug ip interface** command.

Syntax

```
debug ip packet interface {<interface-name>|all} [address
<ip-address>|verbose|hex|arp|udp|tcp|icmp]
```

```
no debug ip packet interface [<interface-name>]
```

Parameter	Description
<interface>	Specify a single Layer 3 interface name (not a range of interfaces) This keyword can be specified as either all or as a single Layer 3 interface to show debugging for either all interfaces or a single interface.
`all`	Specify all Layer 3 interfaces on the device.
<ip-address>	Specify an IPv4 address. If this keyword is specified, then only packets with the specified IP address as specified in the ip-address placeholder are shown in the output.
`verbose`	Specify **verbose** to output more of the IP packet. If this keyword is specified then more of the packet is shown in the output.
`hex`	Specify **hex** to output the IP packet in hexadecimal. If this keyword is specified, then the output for the packet is shown in hex.
`arp`	Specify **arp** to output ARP protocol packets. If this keyword is specified, then ARP packets are shown in the output.
`udp`	Specify **udp** to output UDP protocol packets. If this keyword is specified then UDP packets are shown in the output.
`tcp`	Specify **tcp** to output TCP protocol packets. If this keyword is specified, then TCP packets are shown in the output.
`icmp`	Specify **icmp** to output ICMP protocol packets. If this keyword is specified, then ICMP packets are shown in the output.

Mode Privileged Exec and Global Configuration

Examples

To turn on ARP packet debugging on `vlan1`, use the command:

```
awplus# debug ip packet interface vlan1 arp
```

To turn on all packet debugging on all interfaces on the device, use the command:

```
awplus# debug ip packet interface all
```

To turn on TCP packet debugging on `vlan1` and IP address `192.168.2.4`, use the command:

```
awplus# debug ip packet interface vlan1 address 192.168.2.4 tcp
```

To turn off IP packet interface debugging on all interfaces, use the command:

```
awplus# no debug ip packet interface
```

To turn off IP packet interface debugging on interface `vlan2`, use the command:

```
awplus# no debug ip packet interface vlan2
```

Related Commands

no debug all

show debugging ip dns forwarding

tcpdump

terminal monitor

undebug ip packet interface

ip address (IP Addressing and Protocol)

Overview This command sets a static IP address on an interface.

The **no** variant of this command removes the IP address from the interface. You cannot remove the primary address when a secondary address is present.

Syntax

```
ip address <ip-addr/prefix-length> [secondary] [label <label>]
no ip address [<ip-addr/prefix-length>] [secondary]
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length you are assigning to the interface.
`secondary`	Secondary IP address.
`label`	Adds a user-defined description of the secondary IP address.
<label>	A user-defined description of the secondary IP address. Valid characters are any printable character and spaces.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Usage To set the primary IP address on the interface, specify only **ip address** *<ip-address/m>*. This overwrites any configured primary IP address. To add additional IP addresses on this interface, use the **secondary** parameter. You must configure a primary address on the interface before configuring a secondary address.

NOTE: *Use **show running-config** interface not **show ip interface brief** when you need to view a secondary address configured on an interface. **show ip interface brief** will only show the primary address not a secondary address for an interface.*

Examples To add the primary IP address `10.10.10.50/24` to the interface `vlan3`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip address 10.10.10.50/24
```

To add the secondary IP address `10.10.11.50/24` to the same interface, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip address 10.10.11.50/24 secondary
```

To add the IP address `10.10.11.50/24` to the local loopback interface `lo`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface lo
awplus(config-if)# ip address 10.10.11.50/24
```

Related Commands

interface (to configure)

show ip interface

show running-config interface

ip directed-broadcast

Overview Use this command to enable flooding of directed broadcast packets into a directly connected subnet. If this command is configured on a VLAN interface, then directed broadcasts received on other VLAN interfaces, destined for the subnet on this VLAN, will be flooded to the subnet broadcast address of this VLAN.

Use the **no** variant of this command to disable **ip directed-broadcast**. When this feature is disabled using the **no** variant of this command, directed broadcasts are not forwarded.

Syntax

```
ip directed-broadcast
no ip directed-broadcast
```

Default The **ip directed-broadcast** command is disabled by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Usage IP directed-broadcast is enabled and disabled per VLAN interface. When enabled a directed broadcast packet is forwarded to an enabled VLAN interface if received on another subnet.

An IP directed broadcast is an IP packet whose destination address is a broadcast address for some IP subnet, but originates from a node that is not itself part of that destination subnet. When a directed broadcast packet reaches a device that is directly connected to its destination subnet, that packet is flooded as a broadcast on the destination subnet.

The **ip directed-broadcast c** ommand controls the flooding of directed broadcasts when they reach target subnets. The command affects the final transmission of the directed broadcast on its destination subnet. It does not affect the transit unicast routing of IP directed broadcasts. If directed broadcast is enabled for an interface, incoming directed broadcast IP packets intended for the subnet assigned to interface will be flooded as broadcasts on that subnet.

If the **no ip directed-broadcast** command is configured for an interface, directed broadcasts destined for the subnet where the interface is attached will be dropped instead of broadcast.

Examples To enable **ip directed-broadcast**, to flood broadcast packets out via the `vlan2` interface, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip directed-broadcast
```

To disable **ip directed-broadcast,** disabling the flooding of broadcast packets via `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip directed-broadcast
```

Related Commands

ip forward-protocol udp

ip helper-address

show running-config

ip dns forwarding

Overview Use this command to enable DNS Relay, the forwarding of incoming DNS queries for IP hostname-to-address translation.

Use the **no** variant of this command to disable the forwarding of incoming DNS queries for IP hostname-to-address translation.

Syntax

```
ip dns forwarding
no ip dns forwarding
```

Default The forwarding of incoming DNS query packets is disabled by default.

Mode Global Configuration

Usage DNS Relay requires that IP domain lookup is enabled. IP domain lookup is enabled by default, but if it has been disabled, you can re-enable it by using the command ip domain-lookup.

See the IP Feature Overview and Configuration Guide for more information about DNS Relay. See the ip dns forwarding dead-time command used with this command.

Examples To enable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding
```

To disable the forwarding of incoming DNS query packets, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding
```

Related Commands

clear ip dns forwarding cache

debug ip dns forwarding

ip dns forwarding cache

ip dns forwarding dead-time

ip dns forwarding retry

ip dns forwarding source-interface

ip dns forwarding timeout

ip name-server

show ip dns forwarding

show ip dns forwarding cache

show ip dns forwarding server

ip dns forwarding cache

Overview Use this command to set the DNS Relay name resolver cache size and cache entry lifetime period. The DNS Relay name resolver cache stores the mappings between domain names and IP addresses.

Use the **no** variant of this command to set the default DNS Relay name resolver cache size and cache entry lifetime period.

Note that the lifetime period of the cache entry can be overwritten by the time-out period of the DNS reply from the DNS server if the time-out period of the DNS reply from the DNS server is smaller than the configured time-out period. The time-out period of the cache entry will only be used when the time-out period of the DNS reply from the DNS server is bigger than the time-out period configured on the device.

Syntax

```
ip dns forwarding cache [size <0-1000>] [timeout <60-3600>]
no ip dns forwarding cache [size|timeout]
```

Parameter	Description
<0-1000>	Number of entries in the DNS Relay name resolver cache.
<60-3600>	Timeout value in seconds.

Default The default cache size is 0 (no entries) and the default lifetime is 1800 seconds.

Mode Global Configuration

Usage See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Examples To set the cache size to `10` entries and the lifetime to `500` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding cache size 10 time 500
```

To set the cache size to the default, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding cache size
```

Related Commands

clear ip dns forwarding cache

debug ip dns forwarding

ip dns forwarding

show ip dns forwarding

show ip dns forwarding cache

ip dns forwarding dead-time

Overview Use this command to set the time period in seconds when the device stops sending any DNS requests to an unresponsive server and all retries set using ip dns forwarding retry are used. This time period is the DNS forwarding dead-time. The device stops sending DNS requests at the DNS forwarding dead-time configured and when all of the retries are used.

Use the **no** variant of this command to restore the default DNS forwarding dead-time value of 3600 seconds.

Syntax

```
ip dns forwarding dead-time <60-43200>
no ip dns forwarding retry
```

Parameter	Description
<60-43200>	Set the DNS forwarding dead-time in seconds. At the dead-time set, the switch stops sending DNS requests to an unresponsive server.

Default The default time to stop sending DNS requests to an unresponsive server is 3600 seconds.

Mode Global Configuration

Usage See the IP Feature Overview and Configuration Guide for more information about DNS Relay. See the ip dns forwarding retry command used with this command.

Examples To set the DNS forwarding retry count to 50 and to set the DNS forwarding dead-time to 1800 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding dead-time 1800
awplus(config)# ip dns forwarding retry 50
```

To reset the DNS retry count to the default of 2 and the DNS forwarding dead-time to the default of 3600, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding dead-time
awplus(config)# no ip dns forwarding retry
```

Related Commands

debug ip dns forwarding

ip dns forwarding

ip dns forwarding retry

show ip dns forwarding

show ip dns forwarding server

ip dns forwarding retry

Overview Use this command to set the number of times DNS Relay will retry to forward DNS queries. The device stops sending DNS requests to an unresponsive server at the time set using the ip dns forwarding dead-time command and when all of the retries are used.

Use the **no** variant of this command to set the number of retries to the default of 2.

Syntax

```
ip dns forwarding retry <0-100>
no ip dns forwarding retry
```

Parameter	Description
<0-100>	Set the number of times DNS Relay will retry to forward a DNS query.

Default The default number of retries is 2 DNS requests to an unresponsive server.

Mode Global Configuration

Usage See the IP Feature Overview and Configuration Guide for more information about DNS Relay. See the ip dns forwarding dead-time command used with this command.

Examples To set the DNS forwarding retry count to `50` and to set the DNS forwarding dead-time to `1800` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding retry 50
awplus(config)# ip dns forwarding dead-time 1800
```

To reset the DNS retry count to the default of `2` and the DNS forwarding dead-time to the default of `3600` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding retry
awplus(config)# no ip dns forwarding dead-time
```

Related Commands

debug ip dns forwarding

ip dns forwarding

ip dns forwarding dead-time

show ip dns forwarding

ip dns forwarding source-interface

Overview Use this command to set the interface to use for forwarding and receiving DNS queries.

Use the **no** variant of this command to unset the interface used for forwarding and receiving DNS queries.

Syntax

```
ip dns forwarding source-interface <interface-name>
no ip dns forwarding source-interface
```

Parameter	Description
<interface-name>	An alphanumeric string that is the interface name.

Default The default is that no interface is set and the device selects the appropriate source IP address automatically.

Mode Global Configuration

Usage See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Examples To set `vlan1` as the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding source-interface vlan1
```

To clear the source interface for relayed DNS queries, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding source-interface
```

Related Commands

debug ip dns forwarding

ip dns forwarding

show ip dns forwarding

ip dns forwarding timeout

Overview Use this command to set the time period for the DNS Relay to wait for a DNS response.

Use the **no** variant of this command to set the time period to wait for a DNS response to the default of 3 seconds.

Syntax

```
ip dns forwarding timeout <0-3600>
no ip dns forwarding timeout
```

Parameter	Description
<0-3600>	Timeout value in seconds.

Default The default timeout value is 3 seconds.

Mode Global Configuration

Usage See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Examples To set the timeout value to `12` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dns forwarding timeout 12
```

To set the timeout value to the default of `3` seconds, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dns forwarding timeout
```

Related Commands

debug ip dns forwarding

ip dns forwarding

show ip dns forwarding

ip domain-list

Overview This command adds a domain to the DNS list. Domains are appended to incomplete host names in DNS requests. Each domain in this list is tried in turn in DNS lookups. This list is ordered so that the first entry you create is checked first.

The **no** variant of this command deletes a domain from the list.

Syntax

```
ip domain-list <domain-name>
no ip domain-list <domain-name>
```

Parameter	Description
<domain-name>	Domain string, for example “company.com”.

Mode Global Configuration

Usage If there are no domains in the DNS list, then your device uses the domain specified with the ip domain-name command. If any domain exists in the DNS list, then the device does not use the domain set using the **ip domain-name** command.

Example To add the domain `example.net` to the DNS list, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-list example.net
```

Related Commands

ip domain-lookup

ip domain-name

show ip domain-list

ip domain-lookup

Overview This command enables the DNS client on your device. This allows you to use domain names instead of IP addresses in commands. The DNS client resolves the domain name into an IP address by sending a DNS inquiry to a DNS server, specified with the ip name-server command.

The **no** variant of this command disables the DNS client. The client will not attempt to resolve domain names. You must use IP addresses to specify hosts in commands.

Syntax

```
ip domain-lookup
no ip domain-lookup
```

Mode Global Configuration

Usage The client is enabled by default. However, it does not attempt DNS inquiries unless there is a DNS server configured.

For more information about DNS clients, see the IP Feature Overview and Configuration Guide.

If you are using DNS Relay (see the command ip dns forwarding), you must have IP domain lookup enabled.

Examples To enable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-lookup
```

To disable the DNS client on your device, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip domain-lookup
```

Related Commands

ip domain-list

ip domain-name

ip name-server

show hosts

show ip name-server

ip domain-name

Overview This command sets a default domain for the DNS. The DNS client appends this domain to incomplete host-names in DNS requests.

The **no** variant of this command removes the domain-name previously set by this command.

Syntax

```
ip domain-name <domain-name>
no ip domain-name <domain-name>
```

Parameter	Description
<domain-name>	Domain string, for example “company.com”.

Mode Global Configuration

Usage If there are no domains in the DNS list (created using the ip domain-list command) then your device uses the domain specified with this command. If any domain exists in the DNS list, then the device does not use the domain configured with this command.

When your device is using its DHCP client for an interface, it can receive Option 15 from the DHCP server. This option replaces the domain name set with this command.

Example To configure the domain name, enter the following commands:

```
awplus# configure terminal
awplus(config)# ip domain-name company.com
```

Related Commands

ip domain-list

show ip domain-list

show ip domain-name

ip forward-protocol udp

Overview This command enables you to control which UDP broadcasts will be forwarded to the helper address(es). A UDP broadcast will only be forwarded if the destination UDP port number in the packet matches one of the port numbers specified using this command.

Refer to the IANA site (www.iana.org) for a list of assigned UDP port numbers for protocols to forward using **ip forward-protocol udp**.

Use the **no** variant of this command to remove a port number from the list of destination port numbers that are used as the criterion for deciding if a given UDP broadcast should be forwarded to the IP helper address(es).

Syntax

```
ip forward-protocol udp <port>
no ip forward-protocol udp <port>
```

Parameter	Description
<port>	UDP Port Number.

Default The **ip forward-protocol udp** command is not enabled by default.

Mode Global Configuration

Usage Combined with the ip helper-address command in interface mode, the **ip forward-protocol udp** command in Global Configuration mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

NOTE:

*The types of UDP broadcast packets that the device will forward are ONLY those specified by the **ip forward-protocol** command(s). There are no other UDP packet types that the IP helper process forwards by default.*

NOTE:

*The **ip forward-protocol udp** command does not support BOOTP / DHCP Relay. The **ip dhcp-relay** command must be used instead. For this reason, you may not configure UDP ports 67 and 68 with the **ip forward-protocol udp** command.*

See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Examples To configure forwarding of packets on a UDP port, use the following commands:

```
awplus# configure terminal
awplus(config)# ip forward-protocol udp <port>
```

To delete a UDP port from the UDP ports that the device forwards, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip forward-protocol udp <port>
```

Related Commands

ip helper-address

ip directed-broadcast

show running-config

ip gratuitous-arp-link

Overview This command sets the Gratuitous ARP time limit for all switchports. The time limit restricts the sending of Gratuitous ARP packets to one Gratuitous ARP packet within the time in seconds.

NOTE: *This command specifies time between sequences of Gratuitous ARP packets, and time between individual Gratuitous ARP packets occurring in a sequence, to allow legacy support for older devices and interoperation between other devices that are not ready to receive and forward data until several seconds after linkup.*

Additionally, jitter has been applied to the delay following linkup, so Gratuitous ARP packets applicable to a given port are spread over a period of 1 second so are not all sent at once. Remaining Gratuitous ARP packets in the sequence occur after a fixed delay from the first one.

Syntax

```
ip gratuitous-arp-link <0-300>
no ip gratuitous-arp-link
```

Parameter	Description
<0-300>	Specify the minimum time between sequences of Gratuitous ARPs and the fixed time between Gratuitous ARPs occurring in a sequence, in seconds. 0 disables the sending of Gratuitous ARP packets. The default is 8 seconds.

Default The default Gratuitous ARP time limit for all switchports is 8 seconds.

Mode Global Configuration

Usage Every switchport will send a sequence of 3 Gratuitous ARP packets to each VLAN that the switchport is a member of, whenever the switchport moves to the forwarding state. The first Gratuitous ARP packet is sent 1 second after the switchport becomes a forwarding switchport. The second and third Gratuitous ARP packets are each sent after the time period specified by the Gratuitous ARP time limit.

Additionally, the Gratuitous ARP time limit specifies the minimum time between the end of one Gratuitous ARP sequence and the start of another Gratuitous ARP sequence. When a link is flapping, the switchport's state is set to forwarding several times. The Gratuitous ARP time limit is imposed to prevent Gratuitous ARP packets from being sent undesirably often.

Examples To disable the sending of Gratuitous ARP packets, use the commands :

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 0
```

To restrict the sending of Gratuitous ARP packets to one every 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip gratuitous-arp-link 20
```

Validation Commands show running-config

ip helper-address

Overview This command adds a forwarding destination address for IP Helper to enable forwarding of User Datagram Protocol (UDP) broadcasts on an interface.

Use the **no** variant of this command to disable the forwarding of broadcast packets to specific addresses.

Syntax

```
ip helper-address <ip-addr>
no ip helper-address <ip-addr>
```

Parameter	Description
<ip-addr>	Forwarding destination IP address for IP Helper.

Default The destination address for the **ip helper-address** command is not configured by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Usage Combined with the ip forward-protocol udp command in global configuration mode, the **ip helper-address** command in interface mode allows control of which protocols (destination port numbers) are forwarded. The **ip forward-protocol udp** command configures protocols for forwarding, and the **ip helper-address** command configures the destination address(es).

The destination address can be a unicast address or a subnet broadcast address. The UDP destination port is configured separately with the **ip forward-protocol udp** command. If multiple destination addresses are registered then UDP packets are forwarded to each IP address added to an IP Helper. Up to 32 destination addresses may be added using IP Helper.

NOTE:

*The types of UDP broadcast packets that the device will forward are ONLY those specified by the **ip forward-protocol** command(s). There are no other UDP packet types that the IP helper process forwards by default.*

NOTE:

*The **ip helper-address** command does not support BOOTP / DHCP Relay. The **ip dhcp-relay** command must be used instead. For this reason, you may not configure UDP ports 67 and 68 with the **ip forward-protocol** command.*

See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Examples

The following example defines IPv4 address `192.168.1.100` as an IP Helper destination address to which to forward UDP broadcasts received on `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip helper-address 192.168.1.100
```

The following example removes IPv4 address `192.168.1.100` as an IP Helper destination address to which to forward UDP broadcasts received on `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip helper-address 192.168.1.100
```

Validation Commands

show running-config

Related Commands

ip forward-protocol udp

ip directed-broadcast

ip limited-local-proxy-arp

Overview Use this command to enable local proxy ARP, but only for a specified set of IP addresses. This makes the device respond to ARP requests for those IP addresses when the addresses are reachable via the interface you are configuring.

To specify the IP addresses, use the command local-proxy-arp.

Use the **no** variant of this command to disable limited local proxy ARP. This stops your device from intercepting and responding to ARP requests for the specified hosts. This allows the hosts to use MAC address resolution to communicate directly with one another.

Syntax

```
ip limited-local-proxy-arp
no ip limited-local-proxy-arp
```

Default Limited local proxy ARP is disabled by default.

Mode Interface Configuration

Usage This command allows you to stop MAC address resolution for specified hosts. Limited local proxy ARP works by intercepting ARP requests for the specified hosts and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of the other hosts through ARP requests.

Limited local proxy ARP ensures that the specified devices cannot send traffic that bypasses Layer 3 routing on your device. This gives you control over which hosts may communicate with one another.

Example To enable limited local proxy ARP, so that the device makes ARP responses to ARP requests for specified addresses, when the ARP requests are received on VLAN2 and the addresses are routed out VLAN2, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip limited-local-proxy-arp
```

Related Commands ip local-proxy-arp

local-proxy-arp

ip local-proxy-arp

Overview This command allows you to stop MAC address resolution between hosts within a private VLAN edge interface. Local Proxy ARP works by intercepting ARP requests between hosts within a subnet and responding with your device's own MAC address details instead of the destination host's details. This stops hosts from learning the MAC address of other hosts within its subnet through ARP requests.

Local Proxy ARP ensures that devices within a subnet cannot send traffic that bypasses Layer 3 routing on your device. This lets you monitor and filter traffic between hosts in the same subnet, and enables you to have control over which hosts may communicate with one another.

When Local Proxy ARP is operating on an interface, your device does not generate or forward any ICMP-Redirect messages on that interface. This command does not enable proxy ARP on the interface; see the ip proxy-arp command for more information on enabling proxy ARP.

The **no** variant of this command disables Local Proxy ARP to stop your device from intercepting and responding to ARP requests between hosts within a subnet. This allows the hosts to use MAC address resolution to communicate directly with one another. Local Proxy ARP is disabled by default.

Syntax

```
ip local-proxy-arp
no ip local-proxy-arp
```

Default Local proxy ARP is disabled by default

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To enable your device to apply Local Proxy ARP on the interface vlan7, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# ip local-proxy-arp
```

To disable your device to apply Local Proxy ARP on the interface `vlan7`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# no ip local-proxy-arp
```

Related Commands

ip proxy-arp

show arp

show running-config

ip name-server

Overview This command adds IPv4 or IPv6 DNS server addresses. The DNS client on your device sends DNS queries to IP addresses in this list when trying to resolve a host name. Host names cannot be resolved until you have added at least one server to this list. A maximum of three name servers can be added to this list.

The **no** variant of this command removes the specified DNS name-server address.

Syntax

```
ip name-server <ip-addr>
no ip name-server <ip-addr>
```

Parameter	Description
<ip-addr>	The IP address of the DNS server that is being added to the name server list. The address is entered in the form A.B.C.D for an IPv4 address, or in the form X:X::X:X for an IPv6 address.

Mode Global Configuration

Usage To allow the device to operate as a DNS proxy, your device must have learned about a DNS name-server to forward requests to. Name-servers can be learned through the following means:

- Manual configuration, using the **ip name-server** command
- Learned from DHCP server with Option 6
- Learned over a PPP tunnel if the neighbor advertises the DNS server

This command is used to statically configure a DNS name-server for the device to use.

For more information about DHCP and DNS, see the IP Feature Overview and Configuration Guide. For more information about PPP and DNS, see the PPP Feature Overview and Configuration Guide.

Examples To allow a device to send DNS queries to a DNS server with the IPv4 address 10.10.10.5, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 10.10.10.5
```

To enable your device to send DNS queries to a DNS server with the IPv6 address 2001:0db8:010d::1, use the commands:

```
awplus# configure terminal
awplus(config)# ip name-server 2001:0db8:010d::1
```

Related Commands

ip domain-list

ip domain-lookup

ip domain-name

show ip dns forwarding cache

show ip name-server

ip proxy-arp

Overview This command enables Proxy ARP responses to ARP requests on an interface. When enabled, your device intercepts ARP broadcast packets and substitutes its own physical address for that of the remote host. By responding to the ARP request, your device ensures that subsequent packets from the local host are directed to its physical address, and it can then forward these to the remote host.

Your device responds only when it has a specific route to the address being requested, excluding the interface route that the ARP request arrived from. It ignores all other ARP requests. See the ip local-proxy-arp command about enabling your device to respond to other ARP messages.

The **no** variant of this command disables Proxy ARP responses on an interface. Proxy ARP is disabled by default.

Syntax

```
ip proxy-arp
no ip proxy-arp
```

Default Proxy ARP is disabled by default.

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To enable your device to Proxy ARP on the interface `vlan13`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan13
awplus(config-if)# ip proxy-arp
```

To disable your device to Proxy ARP on the interface `vlan13`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan13
awplus(config-if)# no ip proxy-arp
```

Related Commands

arp (IP address MAC)

ip local-proxy-arp

show arp

show running-config

ip redirects

Overview This command enables the device to send ICMP redirects on one or more interfaces.

Use the **no** variant of this command to stop the device from sending ICMP redirects on one or more interfaces.

Syntax

```
ip redirects
no ip redirects
```

Default ICMP redirects are disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage ICMP redirect messages are used to notify hosts that a better route is available to a destination.

ICMP redirects are used when a packet is routed into the device on the same interface that the packet is routed out of the device. ICMP redirects are only sent to packet sources that are directly connected to the device.

Examples To enable the device to send ICMP redirects on interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip redirects
```

To stop the device from sending ICMP redirects on interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip redirects
```

local-proxy-arp

Overview Use this command to specify an IP subnet for use with limited local proxy ARP. When limited local proxy ARP is enabled with the command ip limited-local-proxy-arp, the device will respond to ARP requests for addresses in that subnet.

Use the **no** variant of this command to stop specifying a subnet for use with limited local proxy ARP.

Syntax

```
local-proxy-arp [<ip-add/mask>]
no local-proxy-arp [<ip-add/mask>]
```

Parameter	Description
<ip-add/mask>	The IP subnet to use with limited local proxy ARP, in dotted decimal format (A.B.C.D/M). To specify a single IP address, use a 32-bit mask.

Default No subnets are specified for use with limited local proxy ARP.

Mode Global Configuration

Example To specify limited local proxy ARP for the address 172.22.0.3, use the following commands:

```
awplus# configure terminal
awplus(config)# local-proxy-arp 172.22.0.3/32
```

Related Commands ip limited-local-proxy-arp

ip unreachables

Overview Use this command to enable ICMP (Internet Control Message Protocol) type 3, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax

```
ip unreachables
no ip unreachables
```

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage When a device receives a packet for a destination that is unreachable it returns an ICMP type 3 message, this message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ip unreachables** command, secures your network against this type of probing.

NOTE: *Disabling ICMP destination unreachable messages breaks applications such as traceroute and Path MTU Discovery (PMTUD), which depend on these messages to operate correctly.*

Table 18-1: ICMP type 3 reason codes and description

Code	Description [RFC]
0	Network unreachable [RFC792]
1	Host unreachable [RFC792]
2	Protocol unreachable [RFC792]
3	Port unreachable [RFC792]
4	Fragmentation required, and DF flag set [RFC792]
5	Source route failed [RFC792]
6	Destination network unknown [RFC1122]
7	Destination host unknown [RFC1122]
8	Source host isolated [RFC1122]
9	Network administratively prohibited [RFC768]
10	Host administratively prohibited [RFC869]
11	Network unreachable for Type of Service [RFC908]
12	Host unreachable for Type of Service [RFC938]
13	Communication administratively prohibited [RFC905]

Table 18-1: ICMP type 3 reason codes and description (cont.)

Code	Description [RFC]
14	Host Precedence Violation [RFC1812]
15	Precedence cutoff in effect [RFC1812]

Example To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ip unreachables
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# ip unreachables
```

optimistic-nd

Overview Use this command to enable the optimistic neighbor discovery feature for both IPv4 and IPv6.

Use the **no** variant of this command to disable the optimistic neighbor discovery feature.

Syntax

```
optimistic-nd
no optimistic-nd
```

Default The optimistic neighbor discovery feature is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage The optimistic neighbor discovery feature allows the device, after learning an IPv4 or IPv6 neighbor, to refresh the neighbor before the neighbor is deleted from the hardware L3 switching table. The neighbor is put into the 'stale' state in the software switching table if is it not refreshed, then the 'stale' neighbors are deleted from the hardware L3 switching table.

The optimistic neighbor discovery feature enables the device to sustain L3 traffic switching to a neighbor without interruption. Without the optimistic neighbor discovery feature enabled L3 traffic is interrupted when a neighbor is 'stale' and is then deleted from the L3 switching table.

If a neighbor receiving optimistic neighbor solicitations does not answer optimistic neighbor solicitations with neighbor advertisements, then the neighbor will be put into the 'stale' state, and subsequently deleted from both the software and the hardware L3 switching tables.

Examples To enable the optimistic neighbor discovery feature on `vlan100`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan100
awplus(config-if)# optimistic-nd
```

To disable the optimistic neighbor discovery feature on `vlan100`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan100
awplus(config-if)# no optimistic-nd
```

Validation Commands show running-config

ping

Overview This command sends a query to another IPv4 host (send Echo Request messages).

Syntax

```
ping [ip] <host> [broadcast] [df-bit {yes|no}] [interval
<0-128>] [pattern <hex-data-pattern>] [repeat
{<1-2147483647>|continuous}] [size <36-18024>] [source
<ip-addr>] [timeout <1-65535>] [tos <0-255>]
```

Parameter	Description
<host>	The destination IP address or hostname.
broadcast	Allow pinging of a broadcast address.
df-bit	Enable or disable the do-not-fragment bit in the IP header.
interval *<0-128>*	Specify the time interval in seconds between sending ping packets. The default is 1. You can use decimal places to specify fractions of a second. For example, to ping every millisecond, set the interval to 0.001.
pattern *<hex-data-pattern>*	Specify the hex data pattern.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
continuous	Continuous ping
size *<36-18024>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
source *<ip-addr>*	The IP address of a configured IP interface to use as the source in the IP header of the ping packet.
timeout *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
tos *<0-255>*	The value of the type of service in the IP header.

Mode User Exec and Privileged Exec

Example To ping the IP address 10.10.0.5 use the following command:

```
awplus# ping 10.10.0.5
```

show arp

Overview Use this command to display entries in the ARP routing and forwarding table—the ARP cache contains mappings of IP addresses to physical addresses for hosts. To have a dynamic entry in the ARP cache, a host must have used the ARP protocol to access another host.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show arp [security [interface [<interface-list>]]
show arp [statistics [detail][interface [<interface-list>]]
```

Mode User Exec and Privileged Exec

Usage Running this command with no additional parameters will display all entries in the ARP routing and forwarding table.

Example To display all ARP entries in the ARP cache, use the following command:

```
awplus# show arp
```

Output Figure 18-1: Example output from the **show arp** command

```
awplus#show
arp

IP Address      MAC Address     Interface      Port         Type
192.168.10.2    0015.77ad.fad8  vlan1          port1.0.1    dynamic
192.168.20.2    0015.77ad.fa48  vlan2          port1.0.2    dynamic
192.168.1.100   00d0.6b04.2a42  vlan2          port1.0.6    static
```

Table 19: Parameters in the output of the **show arp** command

Parameter	Meaning
IP Address	IP address of the network device this entry maps to.
MAC Address	Hardware address of the network device.
Interface	Interface over which the network device is accessed.
Port	Physical port that the network device is attached to.
Type	Whether the entry is a static or dynamic entry. Static entries are added using the arp (IP address MAC) command. Dynamic entries are learned from ARP request/reply message exchanges.

Related Commands

arp (IP address MAC)

clear arp-cache

show debugging ip dns forwarding

Overview Use this command to display the DNS Relay debugging status. DNS Relay debugging is set using the **debug ip dns forwarding** command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging ip dns forwarding
```

Mode User Exec and Privileged Exec

Example To display the DNS Relay debugging status, use the command:

```
awplus# show debugging ip dns forwarding
```

Output Figure 18-2: Example output from the **show debugging ip dns forwarding** command

```
awplus#show debugging ip dns forwarding

DNS Relay debugging status:
  debugging is on
```

Related Commands debug ip dns forwarding

show debugging ip packet

Overview Use this command to show the IP interface debugging status. IP interface debugging is set using the **debug ip packet interface** command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging ip packet
```

Mode User Exec and Privileged Exec

Example To display the IP interface debugging status when the terminal monitor off, use the command:

```
awplus# terminal no monitor
awplus# show debug ip packet
```

Output Figure 18-3: Example output from the **show debugging ip packet** command with **terminal monitor** off

```
awplus#terminal no monitor

awplus#show debug ip packet

IP debugging status:

interface all tcp (stopped)

interface vlan1 arp verbose (stopped)
```

Example To display the IP interface debugging status when the terminal monitor is on, use the command:

```
awplus# terminal monitor
awplus# show debug ip packet
```

Output Figure 18-4: Example output from the **show debugging ip packet** command with **terminal monitor** on

```
awplus#terminal monitor

awplus#show debug ip packet

IP debugging status:

interface all tcp (running)

interface vlan1 arp verbose (running)
```

Related Commands

debug ip packet interface

terminal monitor

show hosts

Overview This command shows the default domain, domain list, and name servers configured on your device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show hosts
```

Mode User Exec and Privileged Exec

Example To display the default domain, use the command:

```
awplus# show hosts
```

Output Figure 18-5: Example output from the **show hosts** command

```
awplus#show hosts

Default domain is mycompany.com
Domain list: company.com
Name/address lookup uses domain service
Name servers are 10.10.0.2 10.10.0.88
```

Related Commands

ip domain-list

ip domain-lookup

ip domain-name

ip name-server

show ip dns forwarding

Overview Use this command to display the DNS Relay status.

Syntax

```
show ip dns forwarding
```

Mode User Exec and Privileged Exec

Examples To display the DNS Relay status, use the command:

```
awplus# show ip dns forwarding
```

Output Figure 18-6: Example output from the **show ip dns forwarding** command

```
awplus#show ip dns forwarding

Max-Retry       : 2
Timeout         : 3 second(s)
Dead-Time       : 3600 second(s)
Source-Interface: not specified
DNS Cache       : disabled
```

Related Commands ip dns forwarding

show ip dns forwarding cache

Overview Use this command to display the DNS Relay name resolver cache.

Syntax

```
show ip dns forwarding cache
```

Mode User Exec and Privileged Exec

Example To display the DNS Relay name resolver cache, use the command:

```
awplus# show ip dns forwarding cache
```

Output Figure 18-7: Example output from the **show ip dns forwarding cache** command

```
awplus#show ip dns forwarding cache

Host                                    Address                 Expires Flags
www.example.com                         172.16.1.1.                 180
mail.example.com                        www.example.com             180 CNAME
www.example.com                         172.16.1.1.                 180 REVERSE
mail.example.com                        172.16.1.5.                 180
```

Related Commands ip dns forwarding cache

ip name-server

show ip dns forwarding server

Overview Use this command to display the status of DNS forwarding name servers.

Syntax

```
show ip dns forwarding server
```

Parameter	Description
`forwarding server`	The DNS forwarding name server.

Mode User Exec and Privileged Exec

Examples To display the status of DNS Relay name servers, use the command:

```
awplus# show ip dns forwarding server
```

Output Figure 18-8: Example output from the **show ip dns forwarding server** command

```
awplus#show ip dns forwarding server

Servers            Forwards      Fails     Dead-Time
172.16.1.1              12          0       active
172.16.1.2               6          3         3900
```

Related Commands

ip dns forwarding

ip dns forwarding dead-time

show ip domain-list

Overview This command shows the domains configured in the domain list. The DNS client uses the domains in this list to append incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip domain-list
```

Mode User Exec and Privileged Exec

Example To display the list of domains in the domain list, use the command:

```
awplus# show ip domain-list
```

Output Figure 18-9: Example output from the **show ip domain-list** command

```
awplus#show ip domain-list
alliedtelesis.com
mycompany.com
```

Related Commands

ip domain-list

ip domain-lookup

show ip domain-name

Overview This command shows the default domain configured on your device. When there are no entries in the DNS list, the DNS client appends this domain to incomplete hostnames when sending a DNS inquiry to a DNS server.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip domain-name
```

Mode User Exec and Privileged Exec

Example To display the default domain configured on your device, use the command:

```
awplus# show ip domain-name
```

Output Figure 18-10: Example output from the **show ip domain-name** command

```
awplus#show ip domain-name
alliedtelesis.com
```

Related Commands ip domain-name

ip domain-lookup

show ip interface

Overview Use this command to display information about interfaces and the IP addresses assigned to them. To display information about a specific interface, specify the interface name with the command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip interface [<interface-list>] [brief]
```

Parameter	Description
<interface-list>	The interfaces to display information about. An interface-list can be: • an interface, e.g. `vlan2` • a continuous range of interfaces separated by a hyphen, e.g. `vlan2-8` or `vlan2-vlan5` • a comma-separated list of interfaces or interface ranges, e.g. `vlan2,vlan5,vlan8-10` The specified interfaces must exist.

Mode User Exec and Privileged Exec

Examples To show brief information for the assigned IP address for interface port1.0.2 use the command:

```
awplus# show ip interface port1.0.2 brief
```

To show the IP addresses assigned to vlan2 and vlan3, use the command:

```
awplus# show ip interface vlan2-3 brief
```

Output Figure 18-11: Example output from the **show ip interface brief** command

```
Interface              IP-Address      Status          Protocol
port1.0.2              unassigned      admin up        down
vlan1                  192.168.1.1     admin up        running
vlan2                  192.168.2.1     admin up        running
vlan3                  192.168.3.1     admin up        running
vlan8                  unassigned      admin up        down
```

show ip name-server

Overview This command displays a list of IPv4 and IPv6 DNS server addresses that your device will send DNS requests to. This is a static list configured using the ip name-server command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show ip name-server
```

Mode User Exec and Privileged Exec

Example To display the list of DNS servers that your device sends DNS requests to, use the command:

```
awplus# show ip name-server
```

Output Figure 18-12: Example output from the **show ip name-server** command

```
awplus# show ip name-server
 10.10.0.123
 10.10.0.124
 2001:0db8:010d::1
```

Related Commands ip domain-lookup

ip name-server

show ip sockets

Overview Use this command to display information about the IP or TCP sockets that are present on the device. It includes TCP, UDP listen sockets, displaying associated IP address and port.

The information displayed for established TCP sessions includes the remote IP address, port, and session state. Raw IP protocol listen socket information is also displayed for protocols such as VRRP and ICMP6, which are configured to receive IP packets with the associated protocol number.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip sockets
```

Mode Privileged Exec

Usage Use this command to verify that the socket being used is opening correctly. If there is a local and remote endpoint, a connection is established with the ports indicated.

Note that this command does not display sockets that are used internally for exchanging data between the various processes that exist on the device and are involved in its operation and management. It only displays sockets that are present for the purposes of communicating with other external devices.

Example To display IP sockets currently present on the device, use the command:

```
awplus# show ip sockets
```

Output Figure 18-13: Example output from the **show ip sockets** command

```
Socket information

Not showing 40 local connections
Not showing 7 local listening ports

Typ Local Address           Remote Address          State
tcp 0.0.0.0:111             0.0.0.0:*               LISTEN
tcp 0.0.0.0:80              0.0.0.0:*               LISTEN
tcp 0.0.0.0:23              0.0.0.0:*               LISTEN
tcp 0.0.0.0:443             0.0.0.0:*               LISTEN
tcp 0.0.0.0:4743            0.0.0.0:*               LISTEN
tcp 0.0.0.0:873             0.0.0.0:*               LISTEN
```

```
tcp :::23                       :::*                    LISTEN
udp 0.0.0.0:111                 0.0.0.0:*
udp 226.94.1.1:5405             0.0.0.0:*
udp 0.0.0.0:161                 0.0.0.0:*
udp :::161                      :::*
raw 0.0.0.0:112                 0.0.0.0:*               112
raw :::58                       :::*                    58
raw :::112                      :::*                    112
```

Table 20: Parameters in the output of the **show ip sockets** command

Parameter	Description
`Not showing <number> local connections`	This field refers to established sessions between processes internal to the device, that are used in its operation and management. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
`Not showing <number> local listening ports`	This field refers to listening sockets belonging to processes internal to the device, that are used in its operation and management. They are not available to receive data from other devices. These sessions are not displayed as they are not useful to the user. <number> is some positive integer.
`Typ`	This column displays the type of the socket. Possible values for this column are: `tcp` : IP Protocol 6 `udp` : IP Protocol 17 `raw` : Indicates that socket is for a non port-orientated protocol (i.e. a protocol other than TCP or UDP) where all packets of a specified IP protocol type are accepted. For raw socket entries the protocol type is indicated in subsequent columns.
`Local Address`	For TCP and UDP listening sockets this shows the destination IP address (either IPv4 or IPv6) and destination TCP or UDP port number for which the socket will receive packets. The address and port are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. For active TCP sessions the IP address will display which of the devices addresses the session was established with. For raw sockets this displays the IP address and IP protocol for which the socket will accept IP packets. The address and protocol are separated by ':'. If the socket will accept packets addressed to any of the device's IP addresses, the IP address will be 0.0.0.0 for IPv4 and :: for IPv6. IP Protocol assignments are described at:www.iana.org/assignments/protocol-numbers

Table 20: Parameters in the output of the **show ip sockets** command (cont.)

Parameter	Description
`Remote Address`	For TCP and UDP listening sockets this shows the source IP address (either IPv4 or IPv6) and source TCP or UDP port number for which the socket will accept packets. The address and port are separated by ':'. If the socket will accept packets addressed from any IP address, the IP address will be 0.0.0.0 for IPv4 or :: for IPv6. This is the usual case for a listening socket. Normally for a listen socket any source port will be accepted. This is indicated by ". For active TCP sessions the IP address will display the remote address and port the session was established with. For raw sockets the entry in this column will be 0.0.0.0: or ::: for IPv4 and IPv6, respectively.

`State`	This column shows the state of the socket. For TCP sockets this shows the state of the TCP state machine. For UDP sockets this column is blank. For raw sockets it contains the IP protocol number. The possible TCP states are:
	`LISTEN`
	`SYN-SENT`
	`SYN-RECEIVED`
	`ESTABLISHED`
	`FIN-WAIT-1`
	`FIN-WAIT-2`
	`CLOSE-WAIT`
	`CLOSING`
	`LAST-ACK`
	`TIME-WAIT`
	`CLOSED`
	RFC793 contains the TCP state machine diagram with Section 3.2 describing each of the states.

show ip traffic

Overview Use this command to display statistics regarding IP traffic sent and received by all interfaces on the device, showing totals for IP and IPv6 and then broken down into sub-categories such as TCP, UDP, ICMP and their IPv6 equivalents when appropriate.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip traffic
```

Mode Privileged Exec

Example To display IP traffic statistics, use the command:

```
awplus# show ip traffic
```

Output Figure 18-14: Example output from the **show ip traffic** command

```
IP:
     261998 packets received
     261998 delivered
     261998 sent
     69721 multicast packets received
     69721 multicast packets sent
     23202841 bytes received
     23202841 bytes sent
     7669296 multicast bytes received
     7669296 multicast bytes sent
IPv6:
     28 packets discarded on transmit due to no route
ICMP6:
UDP6:
UDPLite6:
TCP:
     0 remote connections established
     40 local connections established
     7 remote listening ports
     7 local listening ports
     261 active connection openings
     247 passive connection openings
     14 connection attempts failed
     122535 segments received
     122535 segments transmitted
     14 resets transmitted
     227 TCP sockets finished time wait in fast timer
```

```
     155 delayed acks sent
     21187 headers predicted
     736 pure ACKs
     80497 pure ACKs predicted
UDP:
     139468 datagrams received
     139468 datagrams sent
UDPLite:
```

Table 21: Parameters in the output of the **show ip traffic** command

Parameter	Description
IPv4	IPv4 counters
IPv6	IPv6 counters
received packets with no route	Received packets with no route
truncated packets received	Truncated packets received
multicast packets received	Multicast packets received
multicast packets sent	Multicast packets sent
broadcast packets received	Broadcast packets received
broadcast packets sent	Broadcast packets sent
bytes received	Bytes received
bytes sent	Bytes sent
multicast bytes received	Multicast bytes received
multicast bytes sent	Multicast bytes sent
broadcast bytes received	Broadcast bytes received
broadcast bytes sent	Broadcast bytes sent
packets received	Packets received
packets received with invalid headers	Packets received with invalid headers
oversize packets received	Oversize packets received
packets received with no route	Packets received with no route
packets received with invalid address	Packets received with invalid address
packets received with unknown protocol	Packets received with unknown protocol
truncated packets received	Truncated packets received
received packets discarded	Received packets discarded
received packets delivered	Received packets delivered
forwarded packets transmitted	Forwarded packets transmitted

Table 21: Parameters in the output of the **show ip traffic** command (cont.)

Parameter	Description
`packets transmitted`	Packets transmitted
`packets discarded on transmit`	Packets discarded on transmit
`packets discarded on transmit due to no route`	Packets discarded on transmit due to no route
`fragment reassembly timeouts`	Fragment reassembly timeouts
`fragment reassembly required`	Fragment reassembly required
`fragment reassembly OK`	Fragment reassembly OK
`fragment reassembly failures`	Fragment reassembly failures
`fragmentations succeeded`	Fragmentations succeeded
`fragmentations failed`	Fragmentations failed
`fragments created`	Fragments created
`ICMP6`	ICMPv6 counters
`messages received`	Messages received
`errors received`	Errors received
`messages sent`	Messages sent
`TCP`	TCP counters
`remote connections established`	Remote connections established
`local connections established`	Local connections established
`remote listening ports`	Remote listening ports
`local listening ports`	Local listening ports
`active connection openings`	Active connection openings
`passive connection openings`	Passive connection openings
`connection attempts failed`	Connection attempts failed
`connection resets received`	Connection resets received
`segments received`	Segments received
`segments transmitted`	Segments transmitted
`retransmits`	Retransmits
`bad segments received`	Bad segments received
`resets transmitted`	Resets transmitted
`datagrams received`	Datagrams received
`received for unknown port`	Received for unknown port
`datagrams sent`	Datagrams sent
`syncookies sent`	Syncookies sent

Table 21: Parameters in the output of the **show ip traffic** command (cont.)

Parameter	Description
`syncookies received`	Syncookies received
`syncookies failed`	Syncookies failed
`embryonic resets`	Embryonic resets
`sockets pruned`	Sockets pruned
`ICMPs out of window`	ICMPs out of window
`ICMPs dropped due to lock`	ICMPs dropped due to lock
`ARPs filtered`	ARPs filtered
`TCP sockets finished time wait in fast timer`	TCP sockets finished time wait in fast timer
`time wait sockets recycled by time stamp`	Time wait sockets recycled by time stamp
`time wait sockets killed`	Time wait sockets killed
`delayed acks sent`	Delayed acks sent delayed acks further delayed because of locked socket
`delayed acks lost`	Delayed acks lost
`listening socket overflows`	Listening socket overflows
`listening socket drops`	Listening socket drops
`headers predicted`	Headers predicted
`pure ACKs`	Pure ACKs
`pure ACKs predicted`	Pure ACKs predicted
`losses recovered by TCP Reno`	Losses recovered by TCP Reno
`losses recovered by SACK`	Losses recovered by SACK
`SACKs renegged`	SACKs renegged
`detected reordering by FACK`	Detected reordering by FACK
`detected reordering by SACK`	Detected reordering by SACK
`detected reordering by TCP Reno`	Detected reordering by TCP Reno
`detected reordering by sequence`	Detected reordering by sequence
`full undos`	Full undos
`partial undos`	Partial undos
`SACK undos`	SACK undos
`loss undos`	Loss undos
`segments lost`	Segments lost
`lost retransmits`	Lost retransmits

Table 21: Parameters in the output of the **show ip traffic** command (cont.)

Parameter	Description
TCP Reno failures	TCP Reno failures
SACK failures	SACK failures
loss failures	Loss failures
fast retransmits	Fast retransmits
forward retransmits	Forward retransmits
retransmits in slow start	Retransmits in slow start
timeouts	Timeouts
TCP Reno recovery failures	TCP Reno recovery failures
SACK recovery failures	SACK recovery failures
collapsed segments received	Collapsed segments received
DSACKs sent for old packets	DSACKs sent for old packets
DSACKs sent for out of order segments	DSACKs sent for out of order segments
DSACKs received	DSACKs received
DSACKs received for out of order segments	DSACKs received for out of order segments
connections reset due to unexpected SYN	Connections reset due to unexpected SYN
connections reset due to unexpected data	Connections reset due to unexpected data
connections reset due to early user close	Connections reset due to early user close
connections aborted due to lack of memory	Connections aborted due to lack of memory
connections aborted due to timeout	Connections aborted due to timeout
connections aborted due to lingering	Connections aborted due to lingering
connection aborts due to connection failure	Connection aborts due to connection failure
TCP memory pressure events	TCP memory pressure events
SACKs discarded	SACKs discarded
Old DSACKs ignored	Old DSACKs ignored
DSACKs ignored without undo	DSACKs ignored without undo
Spurious RTOs	Spurious RTOs
TCP MD5 Not Found	TCP MD5 Not Found

Table 21: Parameters in the output of the **show ip traffic** command (cont.)

Parameter	Description
`TCP MD5 Unexpected`	TCP MD5 Unexpected
`TCP SACKs shifted`	TCP SACKs shifted
`TCP SACKs merged`	TCP SACKs merged
`TCP SACK shift fallback`	TCP SACK shift fallback
`UDP`	UDP Counters
`UDPLite`	UDPLite Counters
`UDP6`	UDPv6 Counters
`UDPLite6`	UDPLitev6 Counters
`datagrams received`	Datagrams received
`datagrams received for unknown port`	Datagrams received for unknown port
`datagram receive errors`	Datagram receive errors
`datagrams transmitted`	Datagrams transmitted
`datagrams received`	Datagrams received
`datagrams received for unknown port`	Datagrams received for unknown port
`datagram receive errors`	Datagram receive errors
`datagrams transmitted`	Datagrams transmitted

tcpdump

Overview Use this command to start a tcpdump, which gives the same output as the Unix-like **tcpdump** command to display TCP/IP traffic. Press `<ctrl> + c` to stop a running tcpdump.

Syntax

```
tcpdump <line>
```

Parameter	Description
<line>	Specify the dump options. For more information on the options for this placeholder see http://www.tcpdump.org/tcpdump_man.html

Mode Privileged Exec

Example To start a tcpdump running to capture IP packets, enter the command:

```
awplus# tcpdump ip
```

Output Figure 18-15: Example output from the **tcpdump** command

```
03:40:33.221337 IP 192.168.1.1 > 224.0.0.13: PIMv2, Hello,
length: 34
1 packets captured
2 packets received by filter
0 packets dropped by kernel
```

Related Commands debug ip packet interface

traceroute

Overview Use this command to trace the route to the specified IPv4 host.

Syntax `traceroute {<ip-addr>|<hostname>}`

Parameter	Description
<ip-addr>	The destination IPv4 address. The IPv4 address uses the format A.B.C.D.
<hostname>	The destination hostname.

Mode User Exec and Privileged Exec

Example
```
awplus# traceroute 10.10.0.5
```

undebug ip packet interface

Overview This command applies the functionality of the no debug ip packet interface command.

19 IPv6 Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure IPv6. For more information, see the IPv6 Feature Overview and Configuration Guide.

Command List

clear ipv6 neighbors

Overview Use this command to clear all dynamic IPv6 neighbor entries.

Syntax
```
clear ipv6 neighbors
```

Mode Privileged Exec

Example
```
awplus# clear ipv6 neighbors
```

ipv6 address

Overview Use this command to set the IPv6 address of a VLAN interface and enable IPv6.

Use the optional eui64 parameter to derive the interface identifier of the IPv6 address from the MAC address of the interface. Note that the MAC address of the default VLAN is applied if the interface does not have a MAC address of its own when specifying the eui64 parameter.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax

```
ipv6 address <ipv6-addr/prefix-length> [eui64]
no ipv6 address <ipv6-addr/prefix-length> [eui64]
```

Parameter	Description
<ipv6-addr/prefix-length>	Specifies the IPv6 address to be set. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64. Note that your switch will not accept prefix lengths greater than 64.
`eui64`	EUI-64 is a method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch's MAC address. See the Usage section for more information.

Mode Interface Configuration for a VLAN interface.

Usage If the **eui64** parameter is specified then the lower 64 bits of the IPv6 address are appended with the same address that would be acquired through stateless address autoconfiguration (SLAAC) if the device received an RA (Router Advertisement) specifying this prefix. See ipv6 address autoconfig for a detailed command description and examples to enable and disable SLAAC. For more information, see "IPv6 EUI-64 Addressing" in the IPv6 Feature Overview and Configuration Guide.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the ipv6 enable command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command, which was not used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Examples

To assign the IPv6 address 2001:0db8::a2/64 to the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the **eui64** derived address in the prefix `2001:db8::/48` to VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-fr-subif)# ipv6 address 2001:0db8::/48 eui64
```

To remove the **eui64** derived address in the prefix `2001:db8::/48` from VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-fr-subif)# no ipv6 address 2001:0db8::/48 eui64
```

Related Commands

ipv6 address autoconfig

show running-config

show ipv6 interface brief

show ipv6 route

ipv6 address autoconfig

Overview Use this command to enable IPv6 stateless address autoconfiguration (SLAAC) for an interface. This configures an IPv6 address on an interface derived from the MAC address on the interface.

Use the **no** variant of this command to disable IPv6 SLAAC on an interface. Note that if no global addresses are left after removing all IPv6 autoconfigured addresses then IPv6 is disabled.

Syntax

```
ipv6 address autoconfig
no ipv6 address autoconfig
```

Mode Interface Configuration for a VLAN interface.

Usage This command enables automatic configuration of IPv6 addresses using stateless autoconfiguration on an interface and enables IPv6, but does not enable IPv6 forwarding. See the ipv6 forwarding command for further description and examples.

IPv6 hosts can configure themselves when connected to an IPv6 network using ICMPv6 (Internet Control Message Protocol version 6) router discovery messages. Configured routers respond with a Router Advertisement (RA) containing configuration parameters for IPv6 hosts.

The SLAAC process derives the interface identifier of the IPv6 address from the MAC address of the interface. When applying SLAAC to an interface, note that the MAC address of the default VLAN is applied to the interface if the interface does not have its own MAC address.

If SLAAC is not suitable then a network can use stateful configuration with DHCPv6 (Dynamic Host Configuration Protocol version 6) Relay, or hosts can be configured statically. See ip dhcp-relay server-address for the DHCPv6 Relay server command description and examples. See the IP Feature Overview and Configuration Guide for more information about DNS Relay.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them. See the ipv6 enable command for more information.

Also note that the link-local address is retained in the system if the global address is removed using another command that was not used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Examples To enable SLAAC on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address autoconfig
```

To disable SLAAC on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address autoconfig
```

Related Commands

ipv6 address

ipv6 enable

show ipv6 interface brief

show ipv6 route

show running-config

ipv6 enable

Overview Use this command to enable IPv6 on an interface without an IPv6 global address for the interface. This enables IPv6 with a IPv6 link-local address, not an IPv6 global address.

Use the no variant of this command to disable IPv6 on an interface without a global address. Note the **no** variant of this command does not operate on an interface with an IPv6 global address or an interface configured for IPv6 stateless address autoconfiguration (SLAAC).

Syntax

```
ipv6 enable
no ipv6 enable
```

Mode Interface Configuration for a VLAN interface.

Usage The ipv6 enable command automatically configures an IPv6 link-local address on the interface and enables the interface for IPv6 processing.

A link-local address is an IP (Internet Protocol) address that is only used for communications in the local network, or for a point-to-point connection. Routing does not forward packets with link-local addresses. IPv6 requires that a link-local address is assigned to each interface that has the IPv6 protocol enabled, and when addresses are assigned to interfaces for routing IPv6 packets.

Note that link-local addresses are retained in the system until they are negated by using the no variant of the command that established them.

Also note that the link-local address is retained in the system if the global address is removed using another command that was not used to establish the link-local address. For example, if a link local address is established with the ipv6 enable command then it will not be removed using a **no ipv6 address** command.

Examples To enable IPv6 with only a link-local IPv6 address on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
```

To disable IPv6 with only a link-local IPv6 address on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 enable
```

Related Commands

ipv6 address

ipv6 address autoconfig

show ipv6 interface brief

show ipv6 route

show running-config

ipv6 forwarding

Overview Use this command to turn on IPv6 unicast routing for IPv6 packet forwarding.

Execute this command globally on your device prior to issuing ipv6 enable on individual interfaces.

Use this **no** variant of this command to turn off IPv6 unicast routing. Note IPv6 unicast routing is disabled by default.

Syntax

```
ipv6 forwarding
no ipv6 forwarding
```

Mode Global Configuration

Default IPv6 unicast forwarding is disabled by default.

Usage Enable IPv6 unicast forwarding globally for all interface on your device with this command. Use the **no** variant of this command to disable IPv6 unicast forwarding globally for all interfaces on your device.

IPv6 unicast forwarding allows devices to communicate with devices that are more than one hop away, providing that there is a route to the destination address. If IPv6 forwarding is not enabled then pings to addresses on devices that are more than one hop away will fail, even if there is a route to the destination address.

Examples To enable IPv6 unicast routing, use this command as shown below:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
```

To disable IPv6 unicast routing, use the no variant of this command as shown below:

```
awplus# configure terminal
awplus(config)# no ipv6 forwarding
```

Related Commands ipv6 enable

ipv6 multicast-routing

ipv6 multicast forward-slow-path-packet

Overview Use this command to enable multicast packets to be forwarded to the CPU. Enabling this command will ensure that the layer L3 MTU is set correctly for each IP multicast group and will apply the value of the smallest MTU among the outgoing interfaces for the multicast group.

It will also ensure that a received packet that is larger than the MTU value will result in the generation of an ICMP Too Big message.

Use the **no** variant of this command to disable the above functionality.

Syntax

```
ipv6 multicast forward-slow-path-packet
no ipv6 multicast forward-slow-path-packet
```

Default Disabled.

Mode Privileged Exec

Example To enable the ipv6 multicast forward-slow-path-packet function, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-slow-path-packet
```

Related Commands show ipv6 forwarding

ipv6 nd managed-config-flag

Overview Use this command to set the managed address configuration flag, contained within the router advertisement field.

Setting this flag indicates the operation of a stateful autoconfiguration protocol such as DHCPv6 for address autoconfiguration, and that address information (i.e. the network prefix) and other (non-address) information can be requested from the device.

An unset flag enables hosts receiving the advertisements to use a stateless autoconfiguration mechanism to establish their IPv6 addresses. The default is flag unset.

Use the **no** variant of this command to reset this command to its default of, flag unset.

Syntax

```
ipv6 nd managed-config-flag
no ipv6 nd managed-config-flag
```

Default Unset

Mode Interface Configuration for a VLAN interface.

Usage Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the managed address configuration flag on the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd managed-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd other-config-flag

ipv6 nd minimum-ra-interval

Overview Use this command in Interface Configuration mode to set a minimum Router Advertisement (RA) interval for a VLAN interface.

Use the **no** variant of this command in Interface Configuration mode to remove the minimum RA interval for a VLAN interface.

Syntax

```
ipv6 nd minimum-ra-interval <seconds>
no ipv6 nd minimum-ra-interval [<seconds>]
```

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 3 to 1350 seconds.

Default The RA interval for a VLAN interface is unset by default.

Mode Interface Configuration for a VLAN interface.

Examples To set the minimum RA interval for the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd minimum-ra-interval 60
```

To remove the minimum RA interval for the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 nd minimum-ra-interval 60
```

Related Commands

ipv6 nd ra-interval

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd other-config-flag

ipv6 nd other-config-flag

Overview Use this command to set the **other** stateful configuration flag (contained within the router advertisement field) to be used for IPv6 address auto-configuration. This flag is used to request the router to provide information in addition to providing addresses.

NOTE:

Setting the ipv6 nd managed-config-flag command implies that the ipv6 nd other-config-flag will also be set.

Use **no** variant of this command to reset the value to the default.

Syntax

```
ipv6 nd other-config-flag
no ipv6 nd other-config-flag
```

Default Unset

Mode Interface Configuration for a VLAN interface.

Usage Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command. This step is included in the example below.

Example To set the IPv6 other-config-flag on the VLAN interface `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd other-config-flag
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd managed-config-flag

ipv6 nd prefix

Overview Use this command in Interface Configuration mode for a VLAN interface to specify the IPv6 prefix information that is advertised by the router advertisement for IPv6 address auto-configuration.

Use the **no** parameter with this command to reset the IPv6 prefix for a VLAN interface in Interface Configuration mode.

Syntax

```
ipv6 nd prefix <ipv6-prefix/length>
ipv6 nd prefix <ipv6-prefix/length> [<valid-lifetime>]
ipv6 nd prefix <ipv6-prefix/length>
<valid-lifetime><preferred-lifetime> [no-autoconfig]
ipv6 nd prefix <ipv6-prefix/length>
<valid-lifetime><preferred-lifetime> off-link [no-autoconfig]
no ipv6 nd prefix [<ipv6-addr/prefix-length>|all]
```

Parameter	Description
<ipv6-prefix/length>	The prefix to be advertised by the router advertisement message. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. The default is X:X::/64.
<valid-lifetime>	The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 0 and 4294967295 seconds. The default is 2592000 (30 days). Note that this period should be set to a value greater than that set for the prefix preferred-lifetime.
<preferred-lifetime>	Specifies theIPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered a current (undeprecated) value. After this period, the command is still valid but should not be used in new communications. Set to a value between 0 and 4294967295 seconds. The default is 604800 seconds (7 days). Note that this period should be set to a value less than that set for the prefix valid-lifetime.
`off-link`	Specify the IPv6 prefix off-link flag. The default is flag set.
`no-autoconfig`	Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration. The default is flag set.
`all`	Specify all IPv6 prefixes associated with the VLAN interface.

Default Valid-lifetime default is 2592000 seconds (30 days). Preferred-lifetime default is 604800 seconds (7 days).

Mode Interface Configuration for a VLAN interface.

Usage This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Examples The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64`.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64
```

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64` with a valid lifetime of 10 days and a preferred lifetime of 5 days.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 432000
```

The following example configures the device to issue router advertisements on the VLAN interface `vlan4`, and advertises the address prefix of `2001:0db8::/64` with a valid lifetime of 10 days, a preferred lifetime of 5 days and no prefix used for autoconfiguration.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd prefix 2001:0db8::/64 864000 43200
no-autoconfig
```

The following example resets router advertisements on the VLAN interface `vlan4`, so the address prefix of `2001:0db8::/64`is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/64
```

The following example resets all router advertisements on the VLAN interface `vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix all
```

Related Commands ipv6 nd suppress-ra

ipv6 nd ra-interval

Overview Use this command to specify the interval between IPv6 Router Advertisements (RA) transmissions.

Use **no** parameter with this command to reset the value to the default value (600 seconds).

Syntax

```
ipv6 nd ra-interval <seconds>
no ipv6 nd ra-interval
```

Parameter	Description
<seconds>	Specifies the number of seconds between IPv6 Router Advertisements (RAs). Valid values are from 4 to 1800 seconds.

Default 600 seconds.

Mode Interface Configuration for a VLAN interface.

Usage Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command as shown in the example below.

Example To set the advertisements interval on the VLAN interface `vlan4` to be 60 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd ra-interval 60
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd minimum-ra-interval

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd ra-lifetime

Overview Use this command to specify the time period that this router can usefully act as a default gateway for the network. Each router advertisement resets this time period.

Use **no** parameter with this command to reset the value to default.

Syntax

```
ipv6 nd ra-lifetime <seconds>
no ipv6 nd ra-lifetime
```

Parameter	Description
<seconds>	Time period in seconds. Valid values are from 0 to 9000. Note that you should set this time period to a value greater than the value you have set using the ipv6 nd ra-interval command.

Default 1800 seconds

Mode Interface Configuration for a VLAN interface.

Usage This command specifies the lifetime of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command. This instruction is included in the example shown below.

Examples To set the advertisement lifetime of 8000 seconds on the VLAN interface `vlan4`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd ra-lifetime 8000
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd raguard

Overview Use this command to apply the Router Advertisements (RA) Guard feature from the Interface Configuration mode for a device port. This blocks all RA messages received on a device port.

For more information about RA Guard, see the IPv6 Feature Overview and Configuration Guide.

Use the **no** parameter with this command to disable RA Guard for a specified device port.

Syntax

```
ipv6 nd raguard
no ipv6 nd raguard
```

Default RA Guard is not enabled by default.

Mode Interface Configuration for a device port interface.

Usage Router Advertisements (RAs) are used by Routers to announce themselves on the link. Applying RA Guard to a device port disallows Router Advertisements and redirect messages. RA Guard blocks RAs from untrusted hosts. Blocking RAs stops untrusted hosts from flooding malicious RAs and stops any misconfigured hosts from disrupting traffic on the local network.

Enabling RA Guard on a port blocks RAs from a connected host and indicates the port and host are untrusted. Disabling RA Guard on a port allows RAs from a connected host and indicates the port and host are trusted. Ports and hosts are trusted by default to allow RAs.

Example To enable RA Guard on device ports `port1.0.2-1.0.12`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.12
awplus(config-if)# ipv6 nd raguard
```

To verify RA Guard is enabled on device port interface `port1.0.2`, use the command:

```
awplus# show running-config interface port1.0.2
```

To disable RA Guard on device ports `port1.0.2-1.0.12`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-port1.0.12
awplus(config-if)# no ipv6 nd raguard
```

When RA Guard is disabled on a device port it is not displayed in **show running-config** output.

Output Example output from a **show running-config interface** port1.0.2 to verify RA Guard:

```
!
interface port1.0.2
 switchport mode access

 ipv6 nd raguard
!
```

Related Commands show running-config interface

ipv6 nd reachable-time

Overview Use this command to specify the reachable time in the router advertisement to be used for detecting reachability of the IPv6 neighbor.

Use the **no** variant of this command to reset the value to default.

Syntax

```
ipv6 nd reachable-time <milliseconds>
no ipv6 nd reachable-time
```

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000. Setting this value to 0 indicates an unspecified reachable-time.

Default 0 milliseconds

Mode Interface Configuration for a VLAN interface.

Usage This command specifies the reachable time of the current router to be announced in IPv6 Router Advertisements.

Advertisement flags will not be transmitted unless you have applied the ipv6 nd suppress-ra command. This instruction is included in the example shown below.

Example To set the reachable-time in router advertisements on the VLAN interface `vlan4` to be 1800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# ipv6 nd reachable-time 1800000
awplus(config-if)# no ipv6 nd suppress-ra
```

To reset the reachable-time in router advertisements on the VLAN interface `vlan4` to an unspecified reachable-time (0 milliseconds), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd reachable-time
```

Related Commands ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd retransmission-time

Overview Use this command to specify the advertised retransmission interval for Neighbor Solicitation in milliseconds between IPv6 Routers.

Use the **no** variant of this command to reset the retransmission time to the default (1 second).

Syntax

```
ipv6 nd retransmission-time <milliseconds>
no ipv6 nd retransmission-time [<milliseconds>]
```

Parameter	Description
<milliseconds>	Time period in milliseconds. Valid values are from 1000 to 3600000.

Default 1000 milliseconds (1 second)

Mode Interface Configuration for a VLAN interface.

Examples To set the retransmission-time of Neighbor Solicitation on the VLAN interface `vlan2` to be 800000 milliseconds, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 nd retransmission-time 800000
```

To reset the retransmission-time of Neighbor Solicitation on the VLAN interface `vlan2` to the default 1000 milliseconds (1 second), enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 nd retransmission-time
```

Related Commands ipv6 nd suppress-ra

ipv6 nd prefix

ipv6 nd suppress-ra

Overview Use this command to inhibit IPv6 Router Advertisement (RA) transmission for the current interface. Router advertisements are used when applying IPv6 stateless auto-configuration.

Use **no** parameter with this command to enable Router Advertisement transmission.

Syntax

```
ipv6 nd suppress-ra
no ipv6 nd suppress-ra
```

Default Router Advertisement (RA) transmission is suppressed by default.

Mode Interface Configuration for a VLAN interface.

Example To enable the transmission of router advertisements from the VLAN interface `vlan4` on the device, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd suppress-ra
```

Related Commands

ipv6 nd ra-interval

ipv6 nd prefix

ipv6 neighbor

Overview Use this command to add a static IPv6 neighbor entry.

Use the **no** variant of this command to remove a specific IPv6 neighbor entry.

Syntax

```
ipv6 neighbor <ipv6-address> <vlan-name> <mac-address>
<port-list>
```

```
no ipv6 neighbor <ipv6-address> <vlan-name> <port-list>
```

Parameter	Description
<ipv6-address>	Specify the neighbor's IPv6 address in the format X:X::X:X.
<vlan-name>	Specify the neighbor's VLAN name.
<mac-address>	Specify the MAC hardware address in hexadecimal notation in the format `HHHH.HHHH.HHHH`.
<port-list>	Specify the port number, or port range.

Mode Global Configuration

Usage Use this command to clear a specific IPv6 neighbor entry. To clear all dynamic address entries, use the clear ipv6 neighbors command.

Example To create a static neighbor entry for IPv6 address 2001:0db8::a2, on vlan 4, MAC address 0000.cd28.0880, on port1.0.6, use the command:

```
awplus# configure terminal
```

```
awplus(config)# ipv6 neighbor 2001:0db8::a2 vlan4
0000.cd28.0880 port1.0.6
```

Related Commands clear ipv6 neighbors

ipv6 opportunistic-nd

Overview Use this command to enable opportunistic neighbor discovery for the global IPv6 ND cache. Opportunistic neighbor discovery changes the behavior for unsolicited ICMPv6 ND packet forwarding on the device.

Use the **no** variant of this command to disable opportunistic neighbor discovery for the global IPv6 ND cache.

Syntax
```
ipv6 opportunistic-nd
no ipv6 opportunistic-nd
```

Default Opportunistic neighbor discovery is disabled by default.

Mode Global Configuration

Usage When opportunistic neighbor discovery is enabled, the device will reply to any received unsolicited ICMPv6 ND packets. The source MAC address for the unsolicited ICMPv6 ND packet is added to the IPv6 ND cache, so the device forwards the ICMPv6 ND packet. When opportunistic neighbor discovery is disabled, the source MAC address for the ICMPv6 packet is not added to the IPv6 ND cache, so the ICMPv6 ND packet is not forwarded by the device.

Examples To enable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# ipv6 opportunistic-nd
```

To disable opportunistic neighbor discovery for the IPv6 ND cache, enter:

```
awplus# configure terminal
awplus(config)# no ipv6 opportunistic-nd
```

Related Commands arp opportunistic-nd

show ipv6 neighbors

Validation Commands show running-config interface

ipv6 route

Overview Use this command to establish the distance for static routes of a network prefix.

Use the **no** variant of this command to disable the distance for static routes of the network prefix.

Syntax

```
ipv6 route <dest-prefix> <dest-prefix/length>
{<gateway-ip>|<gateway-name>} [<distvalue>]
```

```
no ipv6 route <dest-prefix> <dest-prefix/length>
{<gateway-ip>|<gateway-name>} [<distvalue>]
```

Parameter	Description
<dest-prefix/length>	Specifies the IP destination prefix. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<gateway-ip>	Specifies the IP gateway (or next hop) address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<distvalue>	Specifies the administrative distance for the route. Valid values are from 1 to 255.
<gateway-name>	Specifies the name of the gateway (or next hop) interface.

Mode Global Configuration

Example

```
awplus# configure terminal
awplus(config)# ipv6 route  myintname 322001:0db8::1/128
```

Validation Commands show running-config

show ipv6 route

ipv6 unreachables

Overview Use this command to enable ICMPv6 (Internet Control Message Protocol version 6) type 1, destination unreachable, messages.

Use the **no** variant of this command to disable destination unreachable messages. This prevents an attacker from using these messages to discover the topology of a network.

Syntax

```
ipv6 unreachables
no ipv6 unreachables
```

Default Destination unreachable messages are enabled by default.

Mode Global Configuration

Usage When a device receives a packet for a destination that is unreachable it returns an ICMPv6 type 1 message. This message includes a reason code, as per the table below. An attacker can use these messages to obtain information regarding the topology of a network. Disabling destination unreachable messages, using the **no ipv6 unreachables** command, secures your network against this type of probing.

NOTE: *Disabling ICMPv6 destination unreachable messages breaks applications such as traceroute, which depend on these messages to operate correctly.*

Table 19-1: ICMPv6 type 1 reason codes and description

Code	Description [RFC]
0	No route to destination [RFC4443]
1	Communication with destination administratively prohibited [RFC4443]
2	Beyond scope of source address [RFC4443]
3	Address unreachable [RF4443]
4	Port unreachable [RFC4443]
5	Source address failed ingress/egress policy [RFC4443]
6	Reject route to destination [RFC4443
7	Error in Source Routing Header [RFC6554]

Example To disable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# no ipv6 unreachables
```

To enable destination unreachable messages, use the commands

```
awplus# configure terminal
awplus(config)# ipv6 unreachables
```

ping ipv6

Overview This command sends a query to another IPv6 host (send Echo Request messages).

NOTE: *Use of the interface parameter keyword, plus an interface or an interface range, with this command is only valid when pinging an IPv6 link local address.*

Syntax

```
ping ipv6 {<host>|<ipv6-address>} [repeat
{<1-2147483647>|continuous}] [size <10-1452>] [interface
<interface-list>] [timeout <1-65535>]
```

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
size *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
interface *<interface-list>*	The interface or range of configured IP interfaces to use as the source in the IP header of the ping packet.
timeout *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.
repeat	Specify the number of ping packets to send.
<1-2147483647>	Specify repeat count. The default is 5.
continuous	Continuous ping.
size *<10-1452>*	The number of data bytes to send, excluding the 8 byte ICMP header. The default is 56 (64 ICMP data bytes).
timeout *<1-65535>*	The time in seconds to wait for echo replies if the ARP entry is present, before reporting that no reply was received. If no ARP entry is present, it does not wait.

Mode User Exec and Privileged Exec

Example

```
awplus# ping ipv6 2001:0db8::a2
```

Related Commands traceroute ipv6

show ipv6 forwarding

Overview Use this command to display IPv6 forwarding status.

Syntax

```
show ipv6 forwarding
```

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 forwarding
```

Output Figure 19-1: Example output from the **show ipv6 forwarding** command

```
ipv6 forwarding is on
```

show ipv6 interface brief

Overview Use this command to display brief information about interfaces and the IPv6 address assigned to them.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 interface [brief]
```

Parameter	Description
`brief`	Specify this optional parameter to display brief IPv6 interface information.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ipv6 interface brief
```

Output Figure 19-2: Example output from the **show ipv6 interface brief** command

```
awplus#show ipv6 interface brief
Interface     IPv6-Address                                Status      Protocol
lo            unassigned                                  admin up    running
vlan1         2001:db8::1/48                              admin up    down
              fe80::215:77ff:fee9:5c50/64
```

Related Commands show interface brief

show ipv6 neighbors

Overview Use this command to display all IPv6 neighbors.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 neighbors
```

Mode User Exec and Privileged Exec

show ipv6 route

Overview Use this command to display the IPv6 routing table for a protocol or from a particular table.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 route
[connected|database|static|summary|<ipv6-address>|<ipv6-addr/p
refix-length>)]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`database`	Displays only the IPv6 routing information extracted from the database.
`static`	Displays only the IPv6 static routes you have configured.
`summary`	Displays summary information from the IPv6 routing table.
`<ipv6-address>`	Displays the routes for the specified address in the IP routing table. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`<ipv6-prefix/length>`	Displays only the routes for the specified IP prefix.

Mode User Exec and Privileged Exec

Example 1 To display an IP route with all parameters turned on, use the following command:

```
awplus# show ipv6 route
```

Output Figure 19-3: Example output of the **show ipv6 route** command

```
IPv6 Routing Table
Codes: C - connected, S - staticS   ::/0 [1/0] via
2001::a:0:0:c0a8:a6, vlan10
C   2001:db8::a:0:0:0:0/64 via ::, vlan10
C   2001:db8::14:0:0:0:0/64 via ::, vlan20
C   2001:db8::0:0:0:0/64 via ::, vlan30
C   2001:db8::28:0:0:0:0/64 via ::, vlan40
C   2001:db8::fa:0:0:0:0/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan250
C   2001:db8::/64 via ::, vlan40
C   2001:db8::/64 via ::, vlan20
C   2001:db8::/64 via ::, vlan10
```

Example 2 To display all database entries for an IP route, use the following command:

```
awplus# show ipv6 route database
```

Output Figure 19-4: Example output of the **show ipv6 route database** command

```
IPv6 Routing Table
Codes: C - connected, S - static       > - selected route, * - FIB
route, p - stale info
Timers: Uptime

S   ::/0 [1/0] via 2001::a:0:0:c0a8:a01 inactive, 6d22h12m
         [1/0] via 2001::fa:0:0:c0a8:fa01 inactive, 6d22h12m
```

show ipv6 route summary

Overview Use this command to display the summary of the current NSM RIB entries.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 route summary
```

Mode User Exec and Privileged Exec

Example To display IP route summary, use the following command:

```
awplus# show ipv6 route summary
```

Output Figure 19-5: Example output from the **show ipv6 route summary** command

```
IPv6 routing table name is Default-IPv6-Routing-Table(0)
IPv6 routing table maximum-paths is 4
RouteSource     Networks
connected       4
FIB              5
```

Related Commands show ip route database

traceroute ipv6

Overview Use this command to trace the route to the specified IPv6 host.

Syntax

```
traceroute ipv6 {<ipv6-addr>|<hostname>}
```

Parameter	Description
<ipv6-addr>	The destination IPv6 address. The IPv6 address uses the format X:X::X:X.
<hostname>	The destination hostname.

Mode User Exec and Privileged Exec

Example To run a traceroute for the IPv6 address 2001:0db8::a2, use the following command:

```
awplus# traceroute ipv6 2001:0db8::a2
```

Related Commands ping ipv6

20 Routing Commands

Introduction

Overview

This chapter provides an alphabetical reference of routing commands that are common across the routing IP protocols.

For more information, see the Route Selection Feature Overview and Configuration Guide.

Command List

ip route

Overview This command adds a static route to the Routing Information Base (RIB). If this route is the best route for the destination, then your device adds it to the Forwarding Information Base (FIB). Your device uses the FIB to advertise routes to neighbors and forward packets.

The **no** variant of this command removes the static route from the RIB and FIB.

Syntax

```
ip route <subnet&mask> {<gateway-ip>|<interface>} [<distance>]
no ip route <subnet&mask> {<gateway-ip>|<interface>}
[<distance>]
```

Parameter	Description
<subnet&mask>	The IPv4 address of the destination subnet defined using either a prefix length or a separate mask specified in one of the following formats: The IPv4 subnet address in dotted decimal notation followed by the subnet mask, also in dotted decimal notation. The IPv4 subnet address in dotted decimal notation, followed by a forward slash, then the prefix length.
<gateway-ip>	The IPv4 address of the gateway device.
<interface>	The interface that connects your device to the network. Enter the name of the VLAN or its VID. You can also enter 'null' as an interface. Specify a 'null' interface to add a null or blackhole route to the device. The gateway IP address or the interface is required.
<distance>	The administrative distance for the static route in the range <1-255>. Static routes by default have an administrative distance of 1.

Mode Global Configuration

Default The default administrative distance for a static route is 1 for priority over non-static routes.

Usage Administrative distance can be modified so static routes do not take priority over other routes.

Specify a 'Null' interface to add a null or blackhole route to the switch. A null or blackhole route is a routing table entry that does not forward packets, so any packets sent to it are dropped.

Examples

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To remove the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with the default administrative distance, use the commands:

```
awplus# configure terminal
awplus(config)# no ip route 192.168.3.0 255.255.255.0 10.10.0.2
```

To specify a null or blackhole route 192.168.4.0/24, so packets forwarded to this route are dropped, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.4.0/24 null
```

To add the destination 192.168.3.0 with the mask 255.255.255.0 as a static route available through the device at "10.10.0.2" with an administrative distance of 128, use the commands:

```
awplus# configure terminal
awplus(config)# ip route 192.168.3.0 255.255.255.0 10.10.0.2
128
```

Related Commands

show ip route

show ip route database

max-fib-routes

Overview This command enables you to control the maximum number of FIB routes configured. It operates by providing parameters that enable you to configure preset maximums and warning message thresholds. The operation of these parameters is explained in the Parameter / Description table shown below.

NOTE: *For static routes use the max-static-routes command.*

Use the **no** variant of this command to set the maximum number of FIB routes to the default of 4294967294 FIB routes.

Syntax

```
max-fib-routes <1-4294967294> [<1-100>|warning-only]
no max-fib-routes
```

Parameter	Description
`max-fib-routes`	This is a the maximum number of routes that can be stored in the device's Forwarding Information dataBase. In practice, other practical system limits would prevent this maximum being reached.
<1-4294967294>	The allowable configurable range for setting the maximum number of FIB-routes.
<1-100>	This parameter enables you to optionally apply a percentage value. This percentage will be based on the maximum number of FIB routes you have specified. This will cause a warning message to appear when your routes reach your specified percentage value. Routes can continue to be added until your configured maximum value is reached.
`warning-only`	This parameter enables you to optionally apply a warning message. If you set this option a warning message will appear if your maximum configured value is reached. Routes can continue to be added until your device reaches either the maximum capacity value of 4294967294, or a practical system limit.

Default The default number of fib routes is the maximum number of fib routes (4294967294).

Mode Global Configuration

Examples To set the maximum number of dynamic routes to 2000 and warning threshold of 75%, use the following commands:

```
awplus# config terminal
awplus(config)# max-fib-routes 2000 75
```

max-static-routes

Overview Use this command to set the maximum number of static routes, excluding FIB (Forwarding Information Base) routes.

NOTE: *For FIB routes use the max-fib-routes command.*

Use the **no** variant of this command to set the maximum number of static routes to the default of 1000 static routes.

Syntax

```
max-static-routes <1-1000>
no max-static-routes
```

Default The default number of static routes is the maximum number of static routes (1000).

Mode Global Configuration

Example To reset the maximum number of static routes to the default maximum, use the command:

```
awplus# configure terminal
awplus(config)# no max-static-routes
```

NOTE: *Static routes are applied before adding routes to the RIB (Routing Information Base). Therefore, rejected static routes will not appear in the running config.*

Related Commands max-fib-routes

maximum-paths

Overview This command enables ECMP on your device, and sets the maximum number of paths that each route has in the Forwarding Information Base (FIB). ECMP is enabled by default.

The **no** variant of this command sets the maximum paths to the default of 4.

Syntax

```
maximum-paths <1-8>
no maximum-paths
```

Parameter	Description
<1-8>	The maximum number of paths that a route can have in the FIB.

Default By default the maximum number of paths is 4.

Mode Global Configuration

Examples To set the maximum number of paths for each route in the FIB to 5, use the command:

```
awplus# configure terminal
awplus(config)# maximum-paths 5
```

To set the maximum paths for a route to the default of 4, use the command:

```
awplus# configure terminal
awplus(config)# no maximum-paths
```

show ip route

Overview Use this command to display routing entries in the FIB (Forwarding Information Base). The FIB contains the best routes to a destination, and your device uses these routes when forwarding traffic. You can display a subset of the entries in the FIB based on protocol.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Syntax

```
show ip route [bgp|connected|ospf|rip|static|<ip-addr>|
<ip-addr/prefix-length>]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`static`	Displays only the static routes you have configured.
<ip-addr>	Displays the routes for the specified address. Enter an IPv4 address.
<ip-addr/prefix-length>	Displays the routes for the specified network. Enter an IPv4 address and prefix length.

Mode User Exec and Privileged Exec

Example To display the static routes in the FIB, use the command:

```
awplus# show ip route static
```

Output Each entry in the output from this command has a code preceding it, indicating the source of the routing entry. The first few lines of the output list the possible codes that may be seen with the route entries.

Typically, route entries are composed of the following elements:

- code
- a second label indicating the sub-type of the route
- network or host ip address
- administrative distance and metric
- next hop ip address
- outgoing interface name
- time since route entry was added

Figure 20-1: Example output from the **show ip route** command

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       * - candidate default

C       3.3.3.0/24 is directly connected, vlan1
C       10.10.31.0/24 is directly connected, vlan2
C       10.70.0.0/24 is directly connected, vlan4
C       33.33.33.33/32 is directly connected, lo
```

To avoid repetition, only selected route entries comprising of different elements are described here:

Connected Route

The connected route entry consists of:

```
C       10.10.31.0/24 is directly connected, vlan2
```

This route entry denotes:

- Route entries for network `10.10.31.0/24` are derived from the IP address of local interface `vlan2`.
- These routes are marked as Connected routes `(C)` and always preferred over routes for the same network learned from other routing protocols.

Related Commands

show ip route database

show ip route database

Overview This command displays the routing entries in the RIB (Routing Information Base).

When multiple entries are available for the same prefix, RIB uses the routes' administrative distances to choose the best route. All best routes are entered into the FIB (Forwarding Information Base). To view the routes in the FIB, use the show ip route command.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Syntax

```
show ip route database [connected|ospf|rip|static]
```

Parameter	Description
`connected`	Displays only the routes learned from connected interfaces.
`static`	Displays only the static routes you have configured.

Mode User Exec and Privileged Exec

Example To display the static routes in the RIB, use the command:

```
awplus# show ip route database static
```

Output Figure 20-2: Example output from the **show ip route database** command

```
Codes: C - connected, S - static, R - RIP, B - BGP
       O - OSPF, IA - OSPF inter area
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
> - selected route, * - FIB route, p - stale info

C    *> 10.10.31.0/24 is directly connected, vlan2
S    *> 10.10.34.0/24 [1/0] via 10.10.31.16, vlan2
C    *> 10.30.0.0/24 is directly connected, vlan6
S    *> 11.22.11.0/24 [1/0] via 10.10.31.16, vlan2
S    *> 16.16.16.16/32 [1/0] via 10.10.31.16, vlan2
C    *> 45.45.45.45/32 is directly connected, lo
C    *> 127.0.0.0/8 is directly connected, lo
```

The routes added to the FIB are marked with a *. When multiple routes are available for the same prefix, the best route is indicated with the > symbol. All unselected routes have neither the * nor the > symbol.

Related Commands show ip route

show ip route summary

Overview This command displays a summary of the current RIB (Routing Information Base) entries.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > output redirection token.

Syntax

```
show ip route summary
```

Mode User Exec and Privileged Exec

Example To display a summary of the current RIB entries, use the command:

```
awplus# show ip route summary
```

Output Figure 20-3: Example output from the **show ip route summary** command

```
IP routing table name is Default-IP-Routing-Table(0)
IP routing table maximum-paths is 4
Route Source    Networks
connected       5
Total           8
```

Related Commands

show ip route

show ip route database

Part 4: Multicast Applications

21 Multicast Commands

Introduction

Overview

This chapter provides an alphabetical reference of generic multicast commands. For commands for particular multicast protocols, see:

- IGMP and IGMP Snooping Commands.
- MLD and MLD Snooping Commands

NOTE: *The IPv6 Multicast addresses shown can be derived from IPv6 unicast prefixes as per RFC 3306.The IPv6 unicast prefix reserved for documentation is 2001:0db8::/32 as per RFC 3849. Using the base /32 prefix the IPv6 multicast prefix for 2001:0db8::/32 is ff3x:20:2001:0db8::/64. Where an RP address is 2001:0db8::1 the embedded RP multicast prefix is ff7x:120:2001:0db8::/96. For ASM (Any-Source Multicast) the IPV6 multicast addresses allocated for documentation purposes are ff0x::0db8:0:0/96 as per RFC 6676. This is a /96 prefix so that it can be used with group IDs as per RFC 3307. These addresses should not be used for practical networks (other than for testing purposes), nor should they appear in any public network.*

The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

Command List

clear ip mroute

Overview Use this command to delete entries from the IPv4 multicast routing table.

NOTE: *If you use this command, you should also use the clear ip igmp group command to clear IGMP group membership records.*

Syntax

```
clear ip mroute {*|<ipv4-group-address>
[<ipv4-source-address>]} [pim sparse-mode]
```

Parameter	Description
*	Deletes all multicast routes.
<ipv4-group-address>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-source-address>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.
pim sparse-mode	Clear specified IPv4 multicast route(s) for PIM Sparse Mode only.

Mode Privileged Exec

Usage When this command is used, the Multicast Routing Information Base (MRIB) clears the IPv4 multicast route entries in its IPv4 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a “clear” message to the multicast protocols. Each multicast protocol has its own “clear” multicast route command. The protocol-specific “clear” command clears multicast routes from PIM Sparse Mode, and also clears the routes from the MRIB.

Examples

```
awplus# clear ip mroute 225.1.1.1 192.168.3.3
awplus# clear ip mroute *
```

Related Commands ip multicast route

show ip mroute

clear ip mroute statistics

Overview Use this command to delete multicast route statistics entries from the IP multicast routing table.

Syntax

```
clear ip mroute statistics {*|<ipv4-group-addr>
[<ipv4-source-addr>]}
```

Parameter	Description
*	All multicast route entries.
<ipv4-group-addr>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.

Mode Privileged Exec

Example

```
awplus# clear ip mroute statistics 225.1.1.2 192.168.4.4
awplus# clear ip mroute statistics *
```

clear ipv6 mroute

Overview Use this command to delete one or more dynamically-added route entries from the IPv6 multicast routing table. You need to do this, for example, if you want to create a static route instead of an existing dynamic route.

Syntax
```
clear ipv6 mroute {*|<ipv6-group-address>
[<ipv6-source-address>]}
```

Parameter	Description
*	Deletes all dynamically-learned IPv6 multicast routes.
<ipv6-group-address>	Group IPv6 address, in hexadecimal notation in the format X.X::X.X.
<ipv6-source-address>	Source IPv6 address, in hexadecimal notation in the format X.X::X.X.

Mode Privileged Exec

Usage When this command is used, the Multicast Routing Information Base (MRIB) clears the relevant IPv6 multicast route entries in its IPv6 multicast route table, and removes the entries from the multicast forwarder. The MRIB sends a "clear" message to the multicast protocols. Each multicast protocol has its own "clear" multicast route command.

This command does not remove static routes from the routing table or the configuration. To remove static routes, use the `no` parameter of the command ipv6 multicast route.

Example
```
awplus# clear ipv6 mroute 2001::2 ff08::1
```

Related Commands ipv6 multicast route

show ipv6 mroute

clear ipv6 mroute statistics

Overview Use this command to delete multicast route statistics entries from the IPv6 multicast routing table.

NOTE: *Static IPv6 multicast routes take priority over dynamic IPv6 multicast routes. Use the clear ipv6 mroute command to clear static IPv6 multicast routes and ensure dynamic IPv6 multicast routes can take over from previous static IPv6 multicast routes.*

Syntax

```
clear ipv6 mroute statistics {*|<ipv6-group-address>
[<ipv6-source-address>]}
```

Parameter	Description
*	All multicast route entries.
<ipv6-group-addr>	Group IPv6 address, in hexadecimal notation in the format X.X::X.X.
<ipv6-source-addr>	Source IPv6 address, in hexadecimal notation in the format X.X::X.X.

Mode Privileged Exec

Examples

```
awplus# clear ipv6 mroute statistics 2001::2 ff08::1
awplus# clear ipv6 mroute statistics *
```

ipv6 multicast forward-slow-path-packet

Overview Use this command to enable multicast packets to be forwarded to the CPU. Enabling this command will ensure that the layer L3 MTU is set correctly for each IP multicast group and will apply the value of the smallest MTU among the outgoing interfaces for the multicast group.

It will also ensure that a received packet that is larger than the MTU value will result in the generation of an ICMP Too Big message.

Use the **no** variant of this command to disable the above functionality.

Syntax

```
ipv6 multicast forward-slow-path-packet
no ipv6 multicast forward-slow-path-packet
```

Default Disabled.

Mode Privileged Exec

Example To enable the ipv6 multicast forward-slow-path-packet function, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-slow-path-packet
```

Related Commands show ipv6 forwarding

debug nsm mcast

Overview Use this command to debug IPv4 events in the Multicast Routing Information Base (MRIB).

Syntax

```
debug nsm mcast
{all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}
```

Parameter	Description
`all`	All IPv4 multicast debugging.
`fib-msg`	Forwarding Information Base (FIB) messages.
`mrt`	Multicast routes.
`mtrace`	Multicast traceroute.
`mtrace-detail`	Multicast traceroute detailed debugging.
`register`	Multicast PIM register messages.
`stats`	Multicast statistics.
`vif`	Multicast interface.

Mode Privileged Exec and Global Configuration

Examples

```
awplus# configure terminal
awplus(config)# debug nsm mcast all
awplus# configure terminal
awplus(config)# debug nsm mcast fib-msg
awplus# configure terminal
awplus(config)# debug nsm mcast mrt
awplus# configure terminal
awplus(config)# debug nsm mcast mtrace
awplus# configure terminal
awplus(config)# debug nsm mcast mtrace-detail
awplus# configure terminal
awplus(config)# debug nsm mcast register
awplus# configure terminal
awplus(config)# debug nsm mcast stat
awplus# configure terminal
awplus(config)# debug nsm mcast vif
```

debug nsm mcast6

Overview Use this command to debug IPv6 events in the Multicast Routing Information Base (MRIB).

Syntax
```
debug nsm mcast6
{all|fib-msg|mrt|mtrace|mtrace-detail|register|stats|vif}
```

Parameter	Description
`all`	All IPv4 multicast debugging.
`fib-msg`	Forwarding Information Base (FIB) messages.
`mif`	Multicast interfaces.
`mrt`	Multicast routes.
`register`	Multicast PIM register messages.
`stats`	Multicast statistics.

Mode Privileged Exec and Global Configuration

Examples
```
awplus# configure terminal
awplus(config)# debug nsm mcast6 all
awplus# configure terminal
awplus(config)# debug nsm mcast6 fib-msg
awplus# configure terminal
awplus(config)# debug nsm mcast6 mif
awplus# configure terminal
awplus(config)# debug nsm mcast6 mrt
awplus# configure terminal
awplus(config)# debug nsm mcast6 register
awplus# configure terminal
awplus(config)# debug nsm mcast6 stats
```

ip mroute

Overview Use this command to inform multicast of the RPF (Reverse Path Forwarding) route to a given IPv4 multicast source.

Use the **no** variant of this command to delete a route to an IPv4 multicast source.

Syntax

```
ip mroute <ipv4-source-address/mask-length>
[bgp|ospf|rip|static] <rpf-address> [<admin-distance>]
```

```
no ip mroute <ipv4-source-address/mask-length>
[bgp|ospf|rip|static]
```

Parameter	Description
<ipv4-source-address/mask-length>	A multicast source IPv4 address and mask length, in dotted decimal notation in the format A.B.C.D/M.
`ospf`	OSPF unicast routing protocol.
`rip`	RIP unicast routing protocol.
`static`	Specifies a static route.
<rpf-address>	A.B.C.D The closest known address on the multicast route back to the specified source. This host IPv4 address can be within a directly connected subnet or within a remote subnet. In the case that the address is in a remote subnet, a lookup is done from the unicast route table to find the next hop address on the path to this host.
<admin-distance>	The administrative distance. Use this to determine whether the RPF lookup selects the unicast or multicast route. Lower distances have preference. If the multicast static route has the same distance as the other RPF sources, the multicast static route takes precedence. The default is `0` and the range available is `0-255`.

Mode Global Configuration

Usage Typically, when a Layer 3 multicast routing protocol is determining the RPF (Reverse Path Forwarding) interface for the path to an IPv4 multicast source, it uses the unicast route table to find the best path to the source. However, in some networks a deliberate choice is made to send multicast via different paths to those used for unicast. In this case, the interface via which a multicast stream from a given source enters a router may not be the same as the interface that connects to the best unicast route to that source.

This command enables the user to statically configure the device with “multicast routes” back to given sources. When performing the RPF check on a stream from a given IPv4 source, the multicast routing protocol will look at these static entries as well as looking into the unicast routing table. The route with the lowest

administrative distance - whether a static “multicast route” or a route from the unicast route table - will be chosen as the RPF route to the source.

Note that in this context the term “multicast route” does not imply a route via which the current router will forward multicast; instead it refers to the route the multicast will have traversed in order to arrive at the current router.

Examples The following example creates a static multicast IPv4 route back to the sources in the `10.10.3.0/24` subnet. The multicast route is via the host `192.168.2.3`, and has an administrative distance of `2`:

```
awplus# configure terminal
awplus(config)# ip mroute 10.10.3.0/24 static 2 192.168.2.3 2
```

The following example creates a static multicast IPv4 route back to the sources in the `192.168.3.0/24`subnet. The multicast route is via the host `10.10.10.50`. The administrative distance on this route has the default value of `0`:

```
awplus# configure terminal
awplus(config)# ip mroute 192.168.3.0/24 10.10.10.50
```

Validation Commands show ip rpf

ip multicast forward-first-packet

Overview Use this command to enable multicast to forward the first multicast packets coming to the device.

Use the **no** variant of this command to disable this feature.

Syntax

```
ip multicast forward-first-packet
no ip multicast forward-first-packet
```

Default By default, this feature is disabled.

Mode Global Configuration

Usage If this command is enabled, the device will forward the first packets in a multicast stream that create the multicast route, possibly causing degradation in the quality of the multicast stream, such as the pixelation of video and audio data.

NOTE: *If you use this command, ensure that the ip igmp snooping command is enabled, the default setting, otherwise the device will not process the first packets of the multicast stream correctly.*

The device will forward the first multicast packets to all interfaces which are on the same VLAN as those which asked for this multicast group.

Examples To enable the forwarding of the first multicast packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast forward-first-packet
```

To disable the forwarding of the first multicast packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast forward-first-packet
```

ip multicast route

Overview Use this command to add an IPv4 static multicast route for a specific multicast source and group IPv4 address to the multicast Routing Information Base (RIB). This IPv4 multicast route is used to forward multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs.

Use the **no** variant of this command to either remove an IPv4 static multicast route set with this command or to remove a specific downstream VLAN interface from an IPv4 static multicast route for a specific multicast source and group IPv4 address.

Syntax

```
ip multicast route <ipv4-source-addr> <ipv4-group-addr>
<upstream-vlan-id> [<downstream-vlan-id>]

no ip multicast route <ipv4-source-addr> <ipv4-group-addr>
[<upstream-vlan-id> <downstream-vlan-id>]
```

Parameter	Description
<ipv4-source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-group-addr>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<upstream-vlan-id>	Upstream VLAN interface on which the multicast packets ingress.
<downstream-vlan-id>	Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent.

Default By default, this feature is disabled.

Mode Global Configuration

Usage Only one multicast route entry per IPv4 address and multicast group can be specified. Therefore, if one entry for a static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists you cannot create a static multicast route with same source IPv4 address, group IPv4 address, upstream VLAN and downstream VLANs. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to timeout or clear the dynamic multicast route with the clear ip mroute command.

To update an existing static multicast route entry with more or a new set of downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To create a blackhole or null route where packets from a specified source and group address coming from an upstream VLAN are dropped rather than

forwarded, do not specify the optional <*downstream-vlan-id*> parameter when entering this command.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the <downstream-vlan-id> parameter when entering the **no** variant of this command.

Examples To create a static multicast route for the multicast source IPv4 address 2.2.2.2 and group IPv4 address 224.9.10.11, specifying the upstream VLAN interface as vlan10 and the downstream VLAN interface as vlan20, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
vlan20
```

To create a blackhole route for the multicast source IPv4 address 2.2.2.2 and group IPv4 address 224.9.10.11, specifying the upstream VLAN interface as vlan10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
```

To create an IPv4 static multicast route for the multicast source IPv4 address 2.2.2.2 and group IP address 224.9.10.11, specifying the upstream VLAN interface as vlan10 and the downstream VLAN range as vlan20-25, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast route 2.2.2.2 224.9.10.11 vlan10
vlan20-25
```

To remove the downstream VLAN 23 from the IPv4 static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
vlan10 vlan23
```

To delete an IPv4 static multicast route for the multicast source IP address 2.2.2.2 and group IP address 224.9.10.11, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast route 2.2.2.2 224.9.10.11
```

Related Commands

clear ip mroute

show ip mroute

ip multicast route-limit

Overview Use this command to limit the number of multicast routes that can be added to an IPv4 multicast routing table.

Use the no variant of this command to return the IPv4 route limit to the default.

Syntax

```
ip multicast route-limit <limit> [<threshold>]
no ip multicast route-limit
```

Parameter	Description
<limit>	*<1-2147483647>* Number of routes.
<threshold>	*<1-2147483647>* Threshold above which to generate a warning message. The mroute warning threshold must not exceed the mroute limit.

Default The default limit and threshold value is 2147483647.

Mode Global Configuration

Usage This command limits the number of multicast IPv4 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Examples

```
awplus# configure terminal
awplus(config)# ip multicast route-limit 34 24
awplus# configure terminal
awplus(config)# no ip multicast route-limit
```

ip multicast wrong-vif-suppression

Overview Use this command to prevent unwanted multicast packets received on an unexpected VLAN being trapped to the CPU.

Use the no variant of this command to disable wrong VIF suppression.

Syntax

```
ip ip multicast wrong-vif-suppression
no ip multicast wrong-vif-suppression
```

Default By default, this feature is disabled.

Mode Global Configuration

Usage Use this command if there is excessive CPU load and multicast traffic is enabled. To confirm that VIF messages are being sent to the CPU use the debug nsm mcast6 command.

Examples To enable the suppression of wrong VIF packets, use the following commands:

```
awplus# configure terminal
awplus(config)# ip multicast wrong-vif-suppression
```

To disable the suppression of wrong VIF packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip multicast wrong-vif-suppression
```

ip multicast-routing

Overview Use this command to turn on/off IPv4 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv4 multicast routing after enabling it. Note the default stated below.

Syntax

```
ip multicast-routing
no ip multicast-routing
```

Default By default, IPv4 multicast routing is off.

Mode Global Configuration

Usage When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT), stops IGMP operation, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

Example

```
awplus# configure terminal
awplus(config)# ip multicast-routing
```

Validation Commands show running-config

ipv6 multicast route

Overview Use this command to add an IPv6 static multicast route for a specific multicast source and group IPv6 address to the multicast Routing Information Base (RIB). This IPv6 multicast route is used to forward IPv6 multicast traffic from a specific source and group ingressing on an upstream VLAN to a single or range of downstream VLANs.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

Use the **no** variant of this command to either remove an IPv6 static multicast route set with this command or to remove a specific downstream VLAN interface from an IPv6 static multicast route for a specific IPv6 multicast source and group address.

Syntax

```
ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr>
<upstream-vlan-id> [<downstream-vlan-id>]
```

```
no ipv6 multicast route <ipv6-source-addr> <ipv6-group-addr>
[<upstream-vlan-id> <downstream-vlan-id>]
```

Parameter	Description
<ipv6-group-addr>	Source IPv6 address, in dotted decimal notation in the format X.X::X.X.
<ipv6-group-addr>	Group IP address, in dotted decimal notation in the format X.X::X.X.
<upstream-vlan-id>	Upstream VLAN interface on which the multicast packets ingress.
<downstream-vlan-id>	Downstream VLAN interface or range of VLAN interfaces to which the multicast packets are sent.

Default By default, no static routes exist.

Mode Global Configuration

Usage Only one multicast route entry per IPv6 address and multicast group can be specified. Therefore, if one entry for an IPv6 static multicast route is configured, PIM will not be able to update this multicast route in any way.

If a dynamic multicast route exists, you cannot create a static multicast route with the same source IPv6 address and group IPv6 address. An error message is displayed and logged. To add a new static multicast route, either wait for the dynamic multicast route to time out or clear the dynamic multicast route with the clear ipv6 mroute command.

To update an existing IPv6 static multicast route entry with new or additional downstream VLANs, you must firstly remove the existing static multicast route and then add the new static multicast route with all downstream VLANs specified. If

you attempt to update an existing static multicast route entry with an additional VLAN or VLANs an error message is displayed and logged.

To create a blackhole or null route where packets from a specified source and group address coming from an upstream VLAN are dropped rather than forwarded, do not specify the optional <*downstream-vlan-id*> parameter when entering this command.

To remove a specific downstream VLAN from an existing static multicast route entry, specify the VLAN you want to remove with the `<downstream-vlan-id>` parameter when entering the **no** variant of this command.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if port1.0.1 and port1.0.14 are ports on an EPSR data VLAN vlan101, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

Output Figure 21-1: Example ipv6 mld snooping mrouter commands when static IPv6 multicast routing is being used and the destination VLAN is an EPSR data VLAN:

```
awplus>enable

awplus#configure terminal

awplus(config)#interface vlan101

awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.1

awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.14
```

See ipv6 mld snooping mrouter for a command description and command examples.

Examples To create an IPv6 static multicast route for the multicast source IPv6 address `2001::1` and group IPv6 address `ff08::1`, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN interface as `vlan20`, use the following commands:

```
awplus# configure terminal

awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
vlan20
```

To create a blackhole route for the IPv6 multicast source IP address 2001::1 and group IP address ff08::1, specifying the upstream VLAN interface as `vlan10`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
```

To create an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, specifying the upstream VLAN interface as `vlan10` and the downstream VLAN range as `vlan20-25`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 multicast route 2001::1 ff08::1 vlan10
vlan20-25
```

To remove the downstream VLAN `23` from the IPv6 static multicast route created with the above command, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route 2001::1 ff08::1 vlan10
vlan23
```

To delete an IPv6 static multicast route for the multicast source IPv6 address 2001::1 and group IPv6 address ff08::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 multicast route 2001::1 ff08::1
```

Related Commands

clear ipv6 mroute

ipv6 mld snooping mrouter

show ipv6 mroute

ipv6 multicast route-limit

Overview Use this command to limit the number of multicast routes that can be added to an IPv6 multicast routing table.

Use the no variant of this command to return the IPv6 route limit to the default.

Syntax

```
ipv6 multicast route-limit <limit> [<threshold>]
no ipv6 multicast route-limit
```

Parameter	Description
<limit>	*<1-2147483647>* Number of routes.
<threshold>	*<1-2147483647>* Threshold above which to generate a warning message. The mroute warning threshold must not exceed the mroute limit.

Default The default limit and threshold value is 2147483647.

Mode Global Configuration

Usage This command limits the number of multicast IPv6 routes (mroutes) that can be added to a router, and generates an error message when the limit is exceeded. If the threshold parameter is set, a threshold warning message is generated when this threshold is exceeded, and the message continues to occur until the number of mroutes reaches the limit set by the limit argument.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 multicast route-limit 34 24
awplus# configure terminal
awplus(config)# no ipv6 multicast route-limit
```

ipv6 multicast-routing

Overview Use this command to turn on/off IPv6 multicast routing on the router; when turned off the device does not perform multicast functions.

Use the **no** variant of this command to disable IPv6 multicast routing after enabling it. Note the default stated below.

Syntax

```
ipv6 multicast-routing
no ipv6 multicast-routing
```

Default By default, IPv6 multicast routing is off.

Mode Global Configuration

Usage When the **no** variant of this command is used, the Multicast Routing Information Base (MRIB) cleans up Multicast Routing Tables (MRT, and stops relaying multicast forwarder events to multicast protocols.

When multicast routing is enabled, the MRIB starts processing any MRT addition/deletion requests, and any multicast forwarding events.

You must enable multicast routing before issuing other multicast commands.

Examples

```
awplus# configure terminal
awplus(config)# ipv6 multicast-routing
awplus# configure terminal
awplus(config)# no ipv6 multicast-routing
```

Validation Commands show running-config

multicast

Overview Use this command to enable a device port to route multicast packets that ingress the port.

Use the **no** variant of this command to stop the device port from routing multicast packets that ingress the port. Note that this does not affect Layer 2 forwarding of multicast packets. If you enter **no multicast** on a port, multicast packets received on that port will not be forwarded to other VLANs, but ports in the same VLANs as the receiving port will still receive the multicast packets.

Syntax

```
multicast
no multicast
```

Default By default, all device ports route multicast packets.

Mode Interface Configuration

Examples

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# multicast
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no multicast
```

Validation Commands show running-config

show ip mroute

Overview Use this command to display the contents of the IPv4 multicast routing (mroute) table.

Syntax

```
show ip mroute [<ipv4-group-addr>] [<ipv4-source-addr>]
[{dense|sparse}] [{count|summary}]
```

Parameter	Description
<ipv4-group-addr>	Group IPv4 address, in dotted decimal notation in the format A.B.C.D.
<ipv4-source-addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.
`dense`	Display dense IPv4 multicast routes.
`sparse`	Display sparse IPv4 multicast routes.
`count`	Display the route and packet count from the IPv4 multicast routing (mroute) table.
`summary`	Display the contents of the IPv4 multicast routing (mroute) table in an abbreviated form.

Mode User Exec and Privileged Exec

Examples

```
awplus# show ip mroute 10.10.3.34 224.1.4.3
awplus# show ip mroute 10.10.5.24 225.2.2.2 count
awplus# show ip mroute 10.10.1.34 summary
```

Output The following is a sample output of this command displaying the IPv4 multicast routing table, with and without specifying the group and source IPv4 address:

Figure 21-2: Example output from the **show ip mroute** command

```
awplus# show ip mroute
IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:00:31, stat expires 00:02:59
Owner PIM-SM, Flags: TF
  Incoming interface: vlan2
  Outgoing interface list:
   vlan3 (1)
```

Figure 21-3: Example output from the **show ip mroute** command with the source and group IPv4 address specified

```
awplus# show ip mroute 10.10.1.52 224.0.1.3

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), uptime 00:03:24, stat expires 00:01:28
Owner PIM-SM, Flags: TF
  Incoming interface: vlan2
  Outgoing interface list:
    vlan3 (1)
```

The following is a sample output of this command displaying the packet count from the IPv4 multicast routing table:

Figure 21-4: Example output from the **show ip mroute count** command

```
awplus# show ip mroute count
IP Multicast Statistics
Total 1 routes using 132 bytes memory
Route limit/Route threshold: 2147483647/2147483647
Total NOCACHE/WRONGVIF/WHOLEPKT recv from fwd: 1/0/0
Total NOCACHE/WRONGVIF/WHOLEPKT sent to clients: 1/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:10

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If
pkts
Fwd msg counts: WRONGVIF/WHOLEPKT recv
Client msg counts: WRONGVIF/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(10.10.1.52, 224.0.1.3), Forwarding: 2/19456, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output for this command displaying the IPv4 multicast routing table in an abbreviated form:

Figure 21-5: Example output from the **show ip mroute summary** command

```
awplus# show ip mroute summary

IP Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface (TTL)

(10.10.1.52, 224.0.1.3), 00:01:32/00:03:20, PIM-SM, Flags: TF
```

show ip mvif

Overview Use this command to display the contents of the IPv4 Multicast Routing Information Base (MRIB) VIF table.

Syntax `show ip mvif [<interface>]`

Parameter	Description
<interface>	The interface to display information about.

Mode User Exec and Privileged Exec

Example `awplus# show ip mvif vlan2`

Output Figure 21-6: Example output from the **show ip mvif** command

```
Interface     Vif   Owner     TTL  Local             Remote          Uptime
              Idx   Module         Address           Address
vlan2         0     PIM-SM    1    192.168.1.53      0.0.0.0         00:04:26
Register      1               1    192.168.1.53      0.0.0.0         00:04:26
vlan3         2     PIM-SM    1    192.168.10.53     0.0.0.0         00:04:25
```

Figure 21-7: Example output from the **show ip mvif** command with the interface parameter **vlan2** specified

```
Interface    Vif   Owner     TTL  Local             Remote           Uptime
             Idx   Module         Address           Address
vlan2        0     PIM-SM    1    192.168.1.53      0.0.0.0          00:05:17
```

show ip rpf

Overview Use this command to display Reverse Path Forwarding (RPF) information for the specified IPv4 source address.

Syntax `show ip rpf <source-addr>`

Parameter	Description
<ipv4-source- addr>	Source IPv4 address, in dotted decimal notation in the format A.B.C.D.

Mode User Exec and Privileged Exec

Example `awplus# show ip rpf 10.10.10.50`

show ipv6 mroute

Overview Use this command to display the contents of the IPv6 multicast routing (mroute) table.

Syntax
```
show ipv6 mroute [<ipv6-group-addr>] [<ipv6-source-addr>]
[{count|summary}]
```

Parameter	Description
<ipv6-group-addr>	Group IPv6 address, in hexadecimal notation in the format X.X::X.X.
<ipv6-source-addr>	Source IPv6 address, in hexadecimal notation in the format X.X::X.X.
`count`	Display the route and packet count from the IPv6 multicast routing (mroute) table.
`summary`	Display the contents of the IPv6 multicast routing (mroute) table in an abbreviated form.

Mode User Exec and Privileged Exec

Examples
```
awplus# show ipv6 mroute
awplus# show ipv6 mroute count
awplus# show ipv6 mroute summary
awplus# show ipv6 mroute 2001::2 ff08::1 count
awplus# show ipv6 mroute 2001::2 ff08::1
awplus# show ipv6 mroute 2001::2 summary
```

Output The following is a sample output of this command displaying the IPv6 multicast routing table for a single static IPv6 Multicast route:

Figure 21-8: Example output from the **show ipv6 mroute** command

```
awplus#show ipv6 mroute
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface
(2001::2, ff08::1), uptime 03:18:38
Owner IMI, Flags: F
  Incoming interface: vlan2
  Outgoing interface list:
    vlan3
```

The following is a sample output of this command displaying the IPv6 multicast routing count table for a single static IPv6 Multicast route:

Figure 21-9: Example output from the **show ipv6 mroute count** command

```
awplus#show ipv6 mroute count

IPv6 Multicast Statistics
Total 1 routes using 152 bytes memory
Route limit/Route threshold: 1024/1024
Total NOCACHE/WRONGmif/WHOLEPKT recv from fwd: 6/0/0
Total NOCACHE/WRONGmif/WHOLEPKT sent to clients: 6/0/0
Immediate/Timed stat updates sent to clients: 0/0
Reg ACK recv/Reg NACK recv/Reg pkt sent: 0/0/0
Next stats poll: 00:01:14

Forwarding Counts: Pkt count/Byte count, Other Counts: Wrong If
pkts
Fwd msg counts: WRONGmif/WHOLEPKT recv
Client msg counts: WRONGmif/WHOLEPKT/Imm Stat/Timed Stat sent
Reg pkt counts: Reg ACK recv/Reg NACK recv/Reg pkt sent

(2001::2, ff08::1), Forwarding: 0/0, Other: 0
  Fwd msg: 0/0, Client msg: 0/0/0/0,  Reg: 0/0/0
```

The following is a sample output of this command displaying the IPv6 multicast routing summary table for a single static IPv6 Multicast route:

Figure 21-10: Example output from the **show ipv6 mroute summary** command

```
awplus#show ipv6 mroute summary
IPv6 Multicast Routing Table
Flags: I - Immediate Stat, T - Timed Stat, F - Forwarder
installed
Timers: Uptime/Stat Expiry
Interface State: Interface

(2001::2, ff08::1), 03:20:28/-, IMI, Flags: F
```

show ipv6 multicast forwarding

Overview Use this command to view the status of multicast forwarding slow-path-packet setting.

Syntax

```
show ipv6 multicast forwarding
```

Mode User Exec

Example To show the status of the multicast forwarding, slow-path-packet setting, use the following command:

```
awplus# show ipv6 multicast forwarding
```

Output Figure 21-11: Example output from the **show ipv6 multicast forwarding** command:

```
ipv6 multicast forwarding is disabled
```

Related Commands ipv6 multicast forward-slow-path-packet

show ipv6 mif

Overview Use this command to display the contents of the IPv6 Multicast Routing Information Base (MRIB) MIF table.

Syntax

```
show ipv6 mif [<interface>]
```

Parameter	Description
<interface>	The interface to display information about.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 mif
awplus# show ipv6 mif vlan2
```

Output Figure 21-12: Example output from the **show ipv6 mif** command

```
awplus#show ipv6 mif
Interface    Mif   Owner             Uptime
             Idx   Module
vlan3        0     MLD/MLD Proxy-Service 03:28:48
vlan2        1     MLD/MLD Proxy-Service 03:28:48
vlan1        2     MLD/MLD Proxy-Service 03:28:48
```

Figure 21-13: Example output from the **show ipv6 mif** command with the interface parameter **vlan2** specified

```
Interface    Mif   Owner     TTL   Remote             Uptime
             Idx   Module          Address
vlan2        0     PIM-SMv6    1     0.0.0.0          00:05:17
```

22 IGMP and IGMP Snooping Commands

Introduction

Overview The Internet Group Management Protocol (IGMP) module includes the IGMP Proxy service and IGMP Snooping functionality. Some of the following commands may have commonalities and restrictions. These are described under the Usage section for each command.

Command List

clear ip igmp

Overview Use this command to clear all IGMP group membership records on all VLAN interfaces.

Syntax
```
clear ip igmp
```

Mode Privileged Exec

Usage This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example
```
awplus# clear ip igmp
```

Validation Commands show ip igmp interface

show running-config

Related Commands clear ip igmp group

clear ip igmp interface

clear ip igmp group

Overview Use this command to clear IGMP group membership records for a specific group on either all VLAN interfaces, a single VLAN interface, or for a range of VLAN interfaces.

Syntax

```
clear ip igmp group *
clear ip igmp group <ip-address> <interface>
```

Parameter	Description
*	Clears all groups on all VLAN interfaces. This is an alias to the clear ip igmp command.
<ip-address>	Specifies the group whose membership records will be cleared from all VLAN interfaces, entered in the form A.B.C.D.
<interface>	Specifies the name of the VLAN interface; all groups learned on this VLAN interface are deleted.

Mode Privileged Exec

Usage This command applies to groups learned by IGMP, IGMP Snooping, or IGMP Proxy.

In addition to the group a VLAN interface can be specified. Specifying this will mean that only entries with the group learned on the interface will be deleted.

Examples

```
awplus# clear ip igmp group *
awplus# clear ip igmp group 224.1.1.1 vlan1
```

Validation Commands show ip igmp interface

show running-config

Related Commands clear ip igmp

clear ip igmp interface

clear ip igmp interface

Overview Use this command to clear IGMP group membership records on a particular VLAN interface.

Syntax

```
clear ip igmp interface <interface>
```

Parameter	Description
<interface>	Specifies the name of the VLAN interface. All groups learned on this VLAN interface are deleted.

Mode Privileged Exec

Usage This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example

```
awplus# clear ip igmp interface vlan1
```

Validation Commands show ip igmp interface

show running-config

Related Commands clear ip igmp

clear ip igmp group

debug igmp

Overview Use this command to enable debugging of either all IGMP or a specific component of IGMP.

Use the **no** variant of this command to disable all IGMP debugging, or debugging of a specific component of IGMP.

Syntax

```
debug igmp {all|decode|encode|events|fsm|tib}
no debug igmp {all|decode|encode|events|fsm|tib}
```

Parameter	Description
`all`	Enable or disable all debug options for IGMP
`decode`	Debug of IGMP packets that have been received
`encode`	Debug of IGMP packets that have been sent
`events`	Debug IGMP events
`fsm`	Debug IGMP Finite State Machine (FSM)
`tib`	Debug IGMP Tree Information Base (TIB)

Modes Privileged Exec and Global Configuration

Usage This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example

```
awplus# configure terminal
awplus(config)# debug igmp all
```

Related Commands show debugging igmp

undebug igmp

ip igmp

Overview Use this command to enable IGMP on an interface. The command configures the device as an IGMP querier.

Use the **no** variant of this command to return all IGMP related configuration to the default on this interface.

Syntax

```
ip igmp
no ip igmp
```

Default Disabled

Mode Interface Configuration for a VLAN interface.

Usage This command can only be configured on VLAN interfaces, and will have no effect on IGMP Proxy or IGMP Snooping configuration.

NOTE: *An IP address must be assigned to the VLAN first, before this command will work.*

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp
```

Validation Commands show ip igmp interface

show running-config

ip igmp access-group

Overview This command adds an access control list to a VLAN interface configured for IGMP, IGMP Snooping, or IGMP Proxy. The access control list is used to control and filter the multicast groups learned on the VLAN interface.

The **no** variant of this command disables the access control filtering on the interface.

Syntax

```
ip igmp access-group {<access-list-number>|<access-list-name>}
no ip igmp access-group
```

Parameter	Description
<access-list-number>	Standard IP access-list number, in the range <1-99>.
<access-list-name>	Standard IP access-list name.

Default By default there are no access lists configured on any interface.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to VLAN interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

This command applies to VLAN interfaces configured for IGMP or IGMP Snooping.

Example In the following example, hosts serviced by VLAN interface vlan2 can only join the group `225.2.2.2`:

```
awplus# configure terminal
awplus(config)# access-list 1 permit 225.2.2.2 0.0.0.0
awplus(config)# interface vlan2
awplus(config-if)# ip igmp access-group 1
```

ip igmp flood specific-query

Overview Use this command if you want IGMP to flood specific queries to all VLAN member ports, instead of only sending the queries to multicast group member ports.

Use the **no** variant of this command if you want IGMP to only send the queries to multicast group member ports.

Syntax

```
ip igmp flood specific-query
no ip igmp flood specific-query
```

Default By default, specific queries are flooded to all VLAN member ports.

Mode Global Configuration

Usage In an L2 switched network running IGMP, it is considered more robust to flood all specific queries. In most cases, the benefit of flooding specific queries to all VLAN member ports outweighs the disadvantages.

However, sometimes this is not the case. For example, if hosts with very low CPU capability receive specific queries for multicast groups they are not members of, their performance may degrade unacceptably. In this situation, it is desirable for IGMP to send specific queries to known member ports only. This minimises the performance degradation of such hosts. In those circumstances, use this command to turn off flooding of specific queries.

Example To cause IGMP to flood specific queries only to multicast group member ports, use the commands:

```
awplus# configure terminal
awplus(config)# no ip igmp flood specific-query
```

Related Commands show ip igmp interface

ip igmp immediate-leave

Overview In IGMP version 2, use this command to minimize the leave latency of IGMP memberships for specified multicast groups. The specified access list number or name defines the multicast groups in which the immediate leave feature is enabled.

Use the **no** variant of this command to disable this feature.

Syntax

```
ip igmp immediate-leave group-list
{<access-list-number>|<access-list-number-expanded>|<access-list-name>}
```

```
no ip igmp immediate-leave
```

Parameter	Description
<access-list-number>	Access-list number, in the range <1-99>.
<access-list-number-expanded>	Access-list number (expanded range), in the range <1300-1999>.
<access-list-name>	Standard IP access-list name.

Default Disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example The following example shows how to enable the immediate-leave feature on the VLAN interface vlan2 for a specific range of multicast groups:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp immediate-leave group-list 34
awplus(config-if)# exit
awplus(config)# access-list 34 permit 225.192.20.0 0.0.0.255
```

Related Commands ip igmp last-member-query-interval

ip igmp last-member-query-count

Overview Use this command to set the last-member query-count value for an interface.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ip igmp last-member-query-count <2-7>
no ip igmp last-member-query-count
```

Parameter	Description
<2-7>	Last member query count value.

Default The default last member query count value is 2.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp last-member-query-count 3
```

Validation Commands show ip igmp interface

show running-config

Related Commands ip igmp last-member-query-interval

ip igmp startup-query-count

ip igmp last-member-query-interval

Overview Use this command to configure the frequency at which the router sends IGMP group specific host query messages.

Use the **no** variant of this command to set this frequency to the default.

Syntax

```
ip igmp last-member-query-interval <interval>
no ip igmp last-member-query-interval
```

Parameter	Description
<interval>	The frequency in milliseconds, in the range <1000-25500>, at which IGMP group-specific host query messages are sent.

Default 1000 milliseconds

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Example The following example changes the IGMP group-specific host query message interval to 2 seconds (2000 milliseconds) for VLAN interface vlan1:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip igmp last-member-query-interval 2000
```

Validation Commands show ip igmp interface

show running-config

Related Commands ip igmp immediate-leave

ip igmp last-member-query-count

ip igmp limit

Overview Use this command to configure the limit on the maximum number of group membership entries for the device as a whole or for the specified interface (if in interface mode). Once the specified number of group memberships is reached, all further membership reports will be ignored. Optionally, you can configure an access-list to stop certain addresses from being subject to the limit.

Use the **no** variant of this command to unset the limit and any specified exception access-list.

Syntax

```
ip igmp limit <limit-value> [except
{<access-list-number>|<access-list-number-extended>|
<access-list-name>}]
```

```
no ip igmp limit
```

Parameter	Description
<limit-value>	Maximum number of group membership entries, from 2 to 512.
<access-list-number>	Access-list number, in the range 1 to 99.
<access-list-number-extended>	Access-list number (expanded range), in the range 1300 to 1999.
<access-list-name>	IP access-list name.

Default The default limit, which is reset by the **no** variant of this command, is 512.

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP, IGMP Snooping, or IGMP Proxy.

Examples The following example configures an IGMP limit of 100 group membership entries on VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp limit 100
```

The following example configures an IGMP limit of 100 group membership entries across all interfaces on which IGMP is enabled, and excludes group `224.1.1.1` from this limitation:

```
awplus# configure terminal
awplus(config)# access-list 1 permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp limit 100 except 1
```

ip igmp mroute-proxy

Overview Use this command to enable IGMP mroute proxy on this downstream interface and associate it with the upstream proxy service interface.

Use the **no** variant of this command to remove the association with the proxy-service interface.

Syntax

```
ip igmp mroute-proxy <interface>
no ip igmp mroute-proxy
```

Parameter	Description
<interface>	The name of the VLAN interface.

Mode Interface Configuration for a VLAN interface.

Usage You must also enable the IGMP proxy service on the upstream interface, using the ip igmp proxy-service command. You can associate one or more downstream mroute proxy interfaces on the device with a single upstream proxy service interface. This downstream mroute proxy interface listens for IGMP reports, and forwards them to the upstream IGMP proxy service interface.

IGMP Proxy does not work with other multicast routing protocols, such as PIM-SM or PIM- DM. This command applies to interfaces configured for IGMP Proxy.

Example The following example configures the VLAN interface `vlan2` as the upstream proxy- service interface for the downstream `vlan3`interface.

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp mroute-proxy vlan2
```

Related Commands ip igmp proxy-service

ip igmp proxy-service

Overview Use this command to enable the VLAN interface to be the upstream IGMP proxy-service interface for the device. All associated downstream IGMP mroute proxy interfaces on this device will have their memberships consolidated on this proxy service interface, according to IGMP host-side functionality.

Use the **no** variant of this command to remove the designation of the VLAN interface as an upstream proxy-service interface.

Syntax

```
ip igmp proxy-service
no ip igmp proxy-service
```

Mode Interface Configuration for a VLAN interface.

Usage This command is used with the ip igmp mroute-proxy command to enable forwarding of IGMP reports to a proxy service interface for all forwarding entries for this interface. You must also enable the downstream IGMP mroute proxy interfaces on this device using the command ip igmp mroute-proxy.

IGMP Proxy does not work with other multicast routing protocols, such as PIM-SM or PIM- DM.

Example The following example designates the VLAN interface `vlan1` as the upstream proxy- service interface.

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip igmp proxy-service
```

Related Commands ip igmp mroute-proxy

ip igmp querier-timeout

Overview Use this command to configure the timeout period before the device takes over as the querier for the VLAN interface after the previous querier has stopped querying.

Use the **no** variant of this command to restore the default.

Syntax

```
ip igmp querier-timeout <timeout>
no ip igmp querier-timeout
```

Parameter	Description
<timeout>	IGMP querier timeout interval value in seconds, in the range <1-65535>.

Default The default timeout interval is 255 seconds.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to VLAN interfaces configured for IGMP. The timeout value should not be less than the current active querier's general query interval.

Example The following example configures the device to wait `130` seconds from the time it received the last query before it takes over as the querier for the VLAN interface vlan20:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp querier-timeout 130
```

Validation Commands show ip igmp interface

show running-config

Related Commands ip igmp query-interval

ip igmp query-holdtime

Overview This command sets the time that an IGMP Querier waits after receiving a query solicitation before it sends an IGMP Query. IGMP General Query messages will not be sent during the hold time interval.

Use the **no** variant of this command to return to the default query hold time period.

Syntax

```
ip igmp query-holdtime <interval>
no ip igmp query-holdtime
```

Parameter	Description
<interval>	Query interval value in milliseconds, in the range <100-5000>.

Default By default the delay before sending IGMP General Query messages is 500 milliseconds.

Mode Interface Configuration for a VLAN interface.

Usage Use this command to configure a value for the IGMP query hold time in the current network. IGMP Queries can be generated after receiving Query Solicitation (QS) packets and there is a possibility of a DoS (Denial of Service) attack if a stream of Query Solicitation (QS) packets are sent to the IGMP Querier, eliciting a rapid stream of IGMP Queries. This command applies to interfaces on which the device is acting as an IGMP Querier.

Use the ip igmp query-interval command when a delay for IGMP general query messages is required and IGMP general query messages are required. The **ip igmp query- holdtime** command stops IGMP query messages during the configured holdtime interval, so the rate of IGMP Queries that can be sent out of an interface can be restricted.

See the IGMP Feature Overview and Configuration Guide for introductory information about the Query Solicitation feature.

NOTE:

This command will function on your device in the stand-alone mode. but is not supported when the device forms part of a VCS Stack.

Examples To set the IGMP query holdtime to `900` ms for `vlan20`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp query-holdtime 900
```

To reset the IGMP query holdtime to the default (500 ms) for `vlan10`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip igmp query-holdtime
```

Validation Commands

show ip igmp interface

show running-config

Related Commands

ip igmp query-interval

ip igmp snooping tcn query solicit

ip igmp query-interval

Overview Use this command to configure the period for sending IGMP General Query messages.

The IGMP query interval specifies the time between IGMP General Query messages being sent.

Use the **no** variant of this command to return to the default query interval period.

NOTE: *The IGMP query interval must be greater than IGMP query maximum response time.*

Syntax

```
ip igmp query-interval <interval>
no ip igmp query-interval
```

Parameter	Description
<interval>	Query interval value in seconds, in the range <2-18000>.

Default The default IGMP query interval is 125 seconds.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP. Note that the IGMP query interval is automatically set to a greater value than the IGMP query max response time.

For example, if you set the IGMP query max response time to 2 seconds using the ip igmp query-max-response-time command, and the IGMP query interval is currently less than 3 seconds, then the IGMP query interval period will be automatically reconfigured to be 3 seconds, so it is greater than the IGMP query maximum response time.

Use the **ip igmp query-interval** command when a non-default interval for IGMP General Query messages is required.

The ip igmp query-holdtime command can occasionally delay the sending of IGMP Queries.

Examples The following example changes the period between IGMP host-query messages to 3 minutes (180 seconds) for VLAN interface vlan20:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp query-interval 180
```

The following example resets the period between sending IGMP host-query messages to the default (125 seconds) for VLAN interface vlan20:

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# no ip igmp query-interval
```

Validation Commands

show ip igmp interface

show running-config

Related Commands

ip igmp query-holdtime

ip igmp query-max-response-time

ip igmp startup-query-interval

ip igmp query-max-response-time

Overview Use this command to configure the maximum response time advertised in IGMP Queries.

Use the **no** variant of this command to restore the default.

NOTE: *The IGMP query maximum response time must be less than the IGMP query interval.*

Syntax

```
ip igmp query-max-response-time <response-time>
no ip igmp query-max-response-time
```

Parameter	Description
<response-time>	Response time value in seconds, in the range <1-3180>.

Default The default IGMP query maximum response time is 10 seconds.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP. Note that the IGMP query interval is automatically set to a greater value than the IGMP query maximum response time.

For example, if you set the IGMP query interval to 3 seconds using the ip igmp query-interval command, and the current IGMP query interval is less than 3 seconds, then the IGMP query maximum response time will be automatically reconfigured to be 2 seconds, so it is less than the IGMP query interval time.

To get the network to converge faster, use the **ip igmp query-max-response-time** command and set a low response time value, such as one or two seconds, so that the clients will respond immediately with a report as a response to the IGMP Queries.

Examples The following example configures a maximum response time of 8 seconds for VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp query-max-response-time 8
```

The following example restores the default maximum response time of 10 seconds for VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp query-max-response-time
```

Validation Commands

show ip igmp interface

show running-config

Related Commands

ip igmp query-interval

ip igmp ra-option (Router Alert)

Overview Use this command to enable strict Router Alert (RA) option validation. With strict RA option enabled, IGMP packets without RA options are ignored.

Syntax

```
ip igmp ra-option
no ip igmp ra-option
```

Default The default state of RA validation is unset.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP and IGMP Snooping.

Example

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp ra-option
```

ip igmp robustness-variable

Overview Use this command to change the robustness variable value on a VLAN interface.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ip igmp robustness-variable <1-7>
no ip igmp robustness-variable
```

Parameter	Description
<1-7>	The robustness variable value.

Default The default robustness variable value is 2.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for IGMP and IGMP Snooping.

Examples

```
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# ip igmp robustness-variable 3
awplus# configure terminal
awplus(config)# interface vlan20
awplus(config-if)# no ip igmp robustness-variable 3
```

Validation Commands show ip igmp interface

show running-config

ip igmp snooping

Overview Use this command to enable IGMP Snooping. When this command is used in the Global Configuration mode, IGMP Snooping is enabled at the device level. When this command is used in Interface Configuration mode, IGMP Snooping is enabled for the specified VLANs.

Use the **no** variant of this command to either globally disable IGMP Snooping, or disable IGMP Snooping on a specified interface.

NOTE: *IGMP snooping cannot be disabled on an interface if IGMP snooping has already been disabled globally. IGMP snooping can be disabled on both an interface and globally if disabled on the interface first and then disabled globally.*

Syntax

```
ip igmp snooping
no ip igmp snooping
```

Default By default, IGMP Snooping is enabled both globally and on all VLANs.

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage For IGMP snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default.)

Both IGMP snooping and MLD snooping must be enabled globally on the device for IGMP snooping to operate. MLD snooping is also enabled by default. To enable it if it has been disabled, use the ipv6 mld snooping command in Global Configuration mode.

Examples

```
awplus# configure terminal
awplus(config)# ip igmp snooping
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping
```

Related Commands

ipv6 mld snooping

show ip igmp interface

show running-config

ip igmp snooping fast-leave

Overview Use this command to enable IGMP Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing. The IGMP group-membership entry is removed as soon as an IGMP leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

Syntax

```
ip igmp snooping fast-leave
no ip igmp snooping fast-leave
```

Default IGMP Snooping fast-leave processing is disabled.

Mode Interface Configuration for a VLAN interface.

Usage This IGMP Snooping command can only be configured on VLAN interfaces.

Example This example shows how to enable fast-leave processing on the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping fast-leave
```

Validation Commands show ip igmp interface

show running-config

ip igmp snooping mrouter

Overview Use this command to statically configure the specified port as a multicast router port for IGMP Snooping for an interface. This command applies to interfaces configured for IGMP Snooping.

Use the **no** variant of this command to remove the static configuration of the port as a multicast router port.

Syntax

```
ip igmp snooping mrouter interface <port>
no ip igmp snooping mrouter interface <port>
```

Parameter	Description
<port>	The port may be a device port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).

Mode Interface Configuration for a VLAN interface.

Example This example shows the switch port interface `port1.0.2` statically configured to be a multicast router interface for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping mrouter interface port1.0.2
```

Related Commands show ip igmp snooping mrouter

ip igmp snooping querier

Overview Use this command to enable IGMP querier operation when no multicast routing protocol is configured. When enabled, the IGMP Snooping querier sends out periodic IGMP queries for all interfaces. This command applies to interfaces configured for IGMP Snooping.

Use the **no** variant of this command to disable IGMP querier configuration.

Syntax
```
ip igmp snooping querier
no ip igmp snooping querier
```

Mode Interface Configuration for a VLAN interface.

Usage The IGMP Snooping querier uses the `0.0.0.0` Source IP address because it only masquerades as a proxy IGMP querier for faster network convergence.

It does not start, or automatically cease, the IGMP Querier operation if it detects query message(s) from a multicast router.

If an IP address is assigned to a VLAN, which has IGMP querier enabled on it, then the IGMP Snooping querier uses the VLAN's IP address as the Source IP Address in IGMP queries.

The IGMP Snooping Querier will not stop sending IGMP Queries if there is another IGMP Snooping Querier in the network with a lower Source IP Address.

NOTE: *Do not enable the IGMP Snooping Querier feature on a Layer 2 device when there is an operational IGMP Querier in the network.*

Example
```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping querier
```

Validation Commands show ip igmp interface

show running-config

ip igmp snooping report-suppression

Overview Use this command to enable report suppression for IGMP versions 1 and 2. This command applies to interfaces configured for IGMP Snooping.

Report suppression stops reports being sent to an upstream multicast router port when there are already downstream ports for this group on this interface.

Use the **no** variant of this command to disable report suppression.

Syntax

```
ip igmp snooping report-suppression
no ip igmp snooping report-suppression
```

Default Report suppression does not apply to IGMPv3, and is turned on by default for IGMPv1 and IGMPv2 reports.

Mode Interface Configuration for a VLAN interface.

Example This example shows how to enable report suppression for IGMPv2 reports for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp version 2
awplus(config-if)# ip igmp snooping report-suppression
```

Validation Commands

show ip igmp interface

show running-config

ip igmp snooping routermode

Overview Use this command to set the destination IP addresses as router multicast addresses.

Use the **no** variant of this command to set it to the default. You can also remove a specified IP address from a custom list of multicast addresses.

Syntax

```
ip igmp snooping routermode
{all|default|ip|multicastrouter|address <ip-address>}
```

```
no ip igmp snooping routermode [address <ip-address>]
```

Parameter	Description
`all`	All reserved multicast addresses (224.0.0.x). Packets from all possible addresses in range 224.0.0.x are treated as coming from routers.
`default`	Default set of reserved multicast addresses. Packets from 224.0.0.1, 224.0.0.2, 224.0.0.4, 224.0.0.5, 224.0.0.6, 224.0.0.9, 224.0.0.13, 224.0.0.15 and 224.0.0.24 are treated as coming from routers.
`ip`	Custom reserved multicast addresses. Packets from custom IP address in the 224.0.0.x range are treated as coming from routers.
`multicastrouter`	Packets from DVMRP (224.0.0.4) and PIM (224.0.0.13) multicast addresses are treated as coming from routers.
`address <ip-address>`	Packets from the specified multicast address are treated as coming from routers. The address must be in the 224.0.0.x range.

Default The default routermode is **default** (not **all**) and shows the following reserved multicast addresses:

```
Router mode.............Def

Reserved multicast address
         224.0.0.1
         224.0.0.2
         224.0.0.4
         224.0.0.5
         224.0.0.6
         224.0.0.9
         224.0.0.13
         224.0.0.15
         224.0.0.24
```

Mode Global Configuration

Examples To set **ip igmp snooping routermode** for all default reserved addresses enter:

```
awplus(config)# ip igmp snooping routermode default
```

To remove the multicast address 224.0.0.5 from the custom list of multicast addresses enter:

```
awplus(config)# no ip igmp snooping routermode address
224.0.0.5
```

Related commands ip igmp trusted

show ip igmp snooping routermode

ip igmp snooping tcn query solicit

Overview Use this command to enable IGMP (Internet Group Management Protocol) Snooping TCN (Topology Change Notification) Query Solicitation feature. When this command is used in the Global Configuration mode, Query Solicitation is enabled.

Use the **no** variant of this command to disable IGMP Snooping TCN Query Solicitation. When the no variant of this command is used in Interface Configuration mode, this overrides the Global Configuration mode setting and Query Solicitation is disabled.

Syntax

```
ip igmp snooping tcn query solicit
no ip igmp snooping tcn query solicit
```

Default IGMP Snooping TCN Query Solicitation is disabled by default on the device, unless the device is the Master Node in an EPSR ring, or is the Root Bridge in a Spanning Tree.

When the device is the Master Node in an EPSR ring, or the device is the Root Bridge in a Spanning Tree, then IGMP Snooping TCN Query Solicitation is enabled by default and cannot be disabled using the Global Configuration mode command. However, Query Solicitation can be disabled for specified VLANs using this command from the Interface Configuration mode. Select the VLAN you want to disable in Interface Configuration mode then issue the no variant of this command to disable the specified VLAN without disabling this feature for other VLANs.

Mode Global Configuration and Interface Configuration for a VLAN interface.

Usage Once enabled, if the device is not an IGMP Querier, on detecting a topology change, the device generates IGMP Query Solicit messages that are sent to all the ports of the vlan configured for IGMP Snooping on the device.

On a device that is not the Master Node in an EPSR ring or the Root Bridge in a Spanning Tree, Query Solicitation can be disabled using the **no** variant of this command after being enabled.

If the device that detects a topology change is an IGMP Querier then the device will generate an IGMP Query message.

Note that the **no** variant of this command when issued in Global Configuration mode has no effect on a device that is the Master Node in an EPSR ring or on a device that is a Root Bridge in a Spanning Tree. Query Solicitation is not disabled for the device these instances. However, Query Solicitation can be disabled on a per-vlan basis from the Interface Configuration mode.

See the below state table that shows when Query Solicit messages are sent in these instances:

Command issued from Global Configuration	Device is STP Root Bridge or the EPSR Master Node	Command issued from Interface Configuration	IGMP Query Solicit message sent on VLAN
No	Yes	Yes	Yes
Yes	Yes	No	No
Yes	Yes	Yes	Yes

See the IGMP Feature Overview and Configuration Guide for introductory information about the Query Solicitation feature.

NOTE:

This command will function on your device in the stand-alone mode. but is not supported when the device forms part of a VCS Stack.

Examples This example shows how to enable IGMP Snooping TCN Query Solicitation on a device:

```
awplus# configure terminal
awplus(config)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation on a device:

```
awplus# configure terminal
awplus(config)# no ip igmp snooping tcn query solicit
```

This example shows how to enable IGMP Snooping TCN Query Solicitation for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp snooping tcn query solicit
```

This example shows how to disable IGMP Snooping TCN Query Solicitation for the VLAN interface vlan2:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp snooping tcn query solicit
```

Validation Commands show ip igmp interface

show running-config

Related Commands ip igmp query-holdtime

ip igmp source-address-check

Overview This command enables the checking of the Source Address for an IGMP Report, rejecting any IGMP Reports originating on devices outside of the local subnet.

Use the **no** variant of this command to disable the checking of the Source Address for an IGMP Report, which allows IGMP Reports from devices outside of the local subnet.

Syntax

```
ip igmp source-address-check
no ip igmp source-address-check
```

Default Source address checking for IGMP Reports is enabled by default.

Mode Interface Configuration for a VLAN interface.

Usage This is a security feature, and should be enabled unless IGMP Reports from outside the local subnet are expected, for example, if Multicast VLAN Registration is active in the network.

The no variant of this command is required to disable the IGMP Report source address checking feature in networks that use Multicast VLAN Registration to allow IGMP Reports from devices outside of the local subnet.

Examples To deny IGMP Reports from outside the current subnet for the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp source-address-check
```

To allow IGMP Reports from outside the current subnet for the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp source-address-check
```

Validation Commands show ip igmp interface

show running-config

ip igmp ssm

Overview Use this command to define a non-default Source Specific Multicast (SSM) range of IP multicast addresses in IGMP. Incoming IGMPv1 and IGMPv2 join requests are ignored if the multicast IP address is in the SSM range and no SSM mapping is configured for these addresses. By default, the SSM range is 232/8. To define the SSM range to be other than the default, use one of the access-list parameter options.

Use the **no** variant of this command to change the SSM range in IGMP back to the default.

Syntax

```
ip igmp ssm range {<access-list-number>|<access-list-name>}
no ip igmp ssm
```

Parameter	Description
<access-list-number>	Access-list number, in the range 1 to 99.
<access-list-name>	Standard IP access-list name.

Default By default the SSM range is 232/8.

Mode Global Configuration

Examples To configure a non-default SSM range to be used in IGMP enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 10 permit 224.1.1.0 0.0.0.255
awplus(config)# ip igmp ssm range 10
```

To return to the default configuration enter the commands:

```
awplus# configure terminal
awplus(config)# no ip igmp ssm
```

ip igmp ssm-map enable

Overview Use this command to enable Source Specific Multicast (SSM) mapping on the device.

Use the **no** variant of this command to disable SSM mapping.

Syntax

```
ip igmp ssm-map enable
no ip igmp ssm-map enable
```

Mode Global Configuration

Usage This command applies to VLAN interfaces configured for IGMP.

Example To enable SSM on the device enter the commands:

```
awplus# configure terminal
awplus(config)# ip igmp ssm-map enable
```

Related Commands ip igmp ssm-map static

ip igmp ssm-map static

Overview Use this command to specify the static mode of defining Source Specific Multicast (SSM) mapping. SSM statically assigns sources to IGMPv1 and IGMPv2 groups to translate such (*,G) groups' memberships to (S,G) memberships for use with PIM-SSM.

Use the **no** variant of this command to remove the SSM map association.

Syntax

```
ip igmp ssm-map static
{<access-list-number>|<access-list-number-extended>|
<access-list-name>} <ip-address>
```

```
no ip igmp ssm-map static
{<access-list-number>|<access-list-number-extended>|
<access-list-name>} <ip-address>
```

Parameter	Description
<access-list-number>	Access-list number, in the range 1 to 99.
<access-list-number-extended>	Access-list number (expanded range), in the range 1300 to 1999.
<access-list-name>	Standard IP access-list name.
<ip-address>	Source address to use for static map group, entered in the form A.B.C.D.

Mode Global Configuration

Usage This command applies to VLAN interfaces configured for IGMP. You can use Standard numbered and Standard named ACLs plus Expanded Numbered ACLs.

Examples This example shows how to configure an SSM static mapping for group-address `224.1.1.1`, using a standard numbered ACL shown as `10`:

```
awplus# configure terminal
awplus(config)# access-list 10 permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp ssm-map static 10 1.2.3.4
```

This example shows how to configure an SSM static mapping for group-address `224.1.1.1`, using an expanded numbered ACL shown as `1301`:

```
awplus# configure terminal
awplus(config)# access-list 1301 permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp ssm-map static 1301 1.2.3.4
```

This example shows how to configure an SSM static mapping for group-address `224.1.1.1`, using a standard named ACL shown as `sales`:

```
awplus# configure terminal
awplus(config)# access-list sales permit 224.1.1.1 0.0.0.0
awplus(config)# ip igmp ssm-map static sales 1.2.3.4
```

Related Commands ip igmp ssm-map enable

ip igmp static-group

Overview Use this command to statically configure multicast group membership entries on a VLAN interface, or to statically forward a multicast channel out a particular port or port range.

To statically add only a group membership, do not specify any parameters.

To statically add a (*,g) entry to forward a channel out of a port, specify only the multicast group address and the switch port range.

To statically add an (s,g) entry to forward a channel out of a port, specify the multicast group address, the source IP address, and the switch port range.

To use Source Specific Multicast mapping to determine the source IP address of the multicast server use the **ssm-map** parameter instead of specifying the source IP address.

Use the **no** variant of this command to delete static group membership entries.

Syntax

```
ip igmp static-group <ip-address> [source
{<ip-source-addr>|ssm-map}] [interface <port>]
```

```
no ip igmp static-group <ip-address> [source
{<ip-source-addr>|ssm-map}] [interface <port>]
```

Parameter	Description
<ip-address>	Standard IP Multicast group address, entered in the form A.B.C.D, to be configured as a static group member.
`source`	Optional.
<ip-source-addr>	Standard IP source address, entered in the form A.B.C.D, to be configured as a static source from where multicast packets originate.
`ssm-map`	This parameter uses Source Specific Multicast (SSM) Mapping to determine the source IP address associated with the specified IP Multicast group address. SSM mappings are configured using the ip igmp ssm-map static command.
`interface`	Use this parameter to specify a specific switch port or switch port range to statically forward the multicast group out of. If not used, static configuration is applied on all ports in the VLAN.
<port>	The port or port range to statically forward the group out of. The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa2`), or a dynamic (LACP) channel group (e.g. `po2`).

Mode Interface Configuration for a VLAN interface.

Usage This command applies to IGMP operation on a specific interface to statically add group and/or source records, or to IGMP Snooping on a VLAN interface to statically add group and/or source records.

Example The following example show how to statically add group and source records for IGMP on the VLAN interface vlan3:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp
awplus(config-if)# ip igmp static-group 226.1.2.4 source
10.2.3.4
```

ip igmp startup-query-count

Overview Use this command to configure the IGMP startup query count for an interface. The IGMP startup query count is the number of IGMP General Query messages sent by a querier at startup. The default IGMP startup query count is 2.

Use the **no** variant of this command to return an interface's configured IGMP startup query count to the default.

Syntax

```
ip igmp startup-query-count <startup-query-count>
no ip igmp startup-query-count
```

Parameter	Description
<startup-query-count>	Specify the IGMP startup query count for a VLAN interface in the range <2-10> where 2 is the default IGMP query count.

Default The default IGMP startup query count is 2.

Mode Interface Configuration for a VLAN interface.

Examples The following example shows how to configure the IGMP startup query count to 4 for the VLAN interface vlan3:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# ip igmp startup-query-count 4
```

The following example shows how to remove the IGMP startup query count for the VLAN interface vlan3:

```
awplus# configure terminal
awplus(config)# interface vlan3
awplus(config-if)# no ip igmp startup-query-count
```

Related Commands ip igmp last-member-query-count

ip igmp startup-query-interval

ip igmp startup-query-interval

Overview Use this command to configure the IGMP startup query interval for an interface. The IGMP startup query interval is the amount of time in seconds between successive IGMP General Query messages sent by a querier during startup. The default IGMP startup query interval is one quarter of the IGMP query interval value.

Use the **no** variant of this command to return an interface's configured IGMP startup query interval to the default.

Syntax

```
ip igmp startup-query-interval <startup-query-interval>
no ip igmp startup-query-interval
```

Parameter	Description
<startup-query-interval>	Specify the IGMP startup query interval for a VLAN interface in Interface Configuration mode in the range of <2-1800> seconds to be one quarter of the IGMP query interval value.

Default The default IGMP startup query interval is one quarter of the IGMP query interval value.

NOTE: *The IGMP startup query interval must be one quarter of the IGMP query interval.*

Mode Interface Configuration for a VLAN interface.

Examples The following example shows how to configure the IGMP startup query interval to `15` seconds for the VLAN interface `vlan2` to be one quarter of the IGMP query interval value of 60 seconds:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ip igmp startup-query-interval 15
awplus(config-if)# ip igmp query-interval 60
```

The following example shows how to remove the IGMP startup query interval for the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip igmp startup-query-interval
```

Related Commands

ip igmp last-member-query-interval

ip igmp query-interval

ip igmp startup-query-count

ip igmp trusted

Overview Use this command to allow IGMP to process packets received on certain trusted ports only.

Use the **no** variant of this command to stop IGMP from processing specified packets if the packets are received on the specified ports or aggregator.

Syntax

```
ip igmp trusted {all|query|report|routermode}
no ip igmp trusted {all|query|report|routermode}
```

Parameter	Description
`all`	Specifies whether or not the interface is allowed to receive all IGMP and other routermode packets
`query`	Specifies whether or not the interface is allowed to receive IGMP queries
`report`	Specifies whether or not the interface is allowed to receive IGMP membership reports
`routermode`	Specifies whether or not the interface is allowed to receive routermode packets

Default By default, all ports and aggregators are trusted interfaces, so IGMP is allowed to process all IGMP query, report, and router mode packets arriving on all interfaces.

Mode Interface mode for one or more switch ports or aggregators

Usage Because all ports are trusted by default, use this command in its **no** variant to stop IGMP processing packets on ports you do not trust.

For example, you can use this command to make sure that only ports attached to approved IGMP routers are treated as router ports.

Example To stop ports port1.0.3-port1.0.6 from being treated as router ports by IGMP, use the commands:

```
awplus(config)# interface port1.0.3-port1.0.6
awplus(config-if)# no ip igmp trusted routermode
```

Related Commands ip igmp snooping routermode

ip igmp version

Overview Use this command to set the current IGMP version (IGMP version 1, 2 or 3) on an interface.

Use the **no** variant of this command to return to the default version.

Syntax

```
ip igmp version <1-3>
no ip igmp version
```

Parameter	Description
<1-3>	IGMP protocol version number

Default The default IGMP protocol version number is 3.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to VLAN interfaces configured for IGMP.

Example

```
awplus# configure terminal
awplus(config)# interface vlan5
awplus(config-if)# ip igmp version 2
```

Validation Commands show ip igmp interface

show debugging igmp

Overview Use this command to display the IGMP debugging options set.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging igmp
```

Mode User Exec and Privileged Exec

Example To display the IGMP debugging options set, enter the command:

```
awplus# show debugging igmp
```

Output Figure 22-1: Example output from the **show debugging igmp** command

```
IGMP Debugging status:
  IGMP Decoder debugging is on
  IGMP Encoder debugging is on
  IGMP Events debugging is on
  IGMP FSM debugging is on
  IGMP Tree-Info-Base (TIB) debugging is on
```

Related Commands debug igmp

show ip igmp groups

Overview Use this command to display the multicast groups with receivers directly connected to the router, and learned through IGMP.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip igmp groups [<ip-address>|<interface> detail]
```

Parameter	Description
<ip-address>	Address of the multicast group, entered in the form A.B.C.D.
<interface>	Interface name for which to display local information.

Mode User Exec and Privileged Exec

Example The following command displays local-membership information for all ports in all interfaces:

```
awplus# show ip igmp groups
```

Output Figure 22-2: Example output from the **show ip igmp groups** command

```
IGMP Connected Group Membership
Group Address    Interface       Uptime    Expires   Last
Reporter
224.0.1.1        port1.0.1       00:00:09  00:04:17  10.10.0.82
224.0.1.24       port1.0.2       00:00:06  00:04:14  10.10.0.84
224.0.1.40       port1.0.3       00:00:09  00:04:15  10.10.0.91
224.0.1.60       port1.0.3       00:00:05  00:04:15  10.10.0.7
224.100.100.100  port1.0.1       00:00:11  00:04:13  10.10.0.91
228.5.16.8       port1.0.3       00:00:11  00:04:16  10.10.0.91
228.81.16.8      port1.0.7       00:00:05  00:04:15  10.10.0.91
228.249.13.8     port1.0.3       00:00:08  00:04:17  10.10.0.91
235.80.68.83     port1.0.11      00:00:12  00:04:15  10.10.0.40
239.255.255.250  port1.0.3       00:00:12  00:04:15  10.10.0.228
239.255.255.254  port1.0.12      00:00:08  00:04:13  10.10.0.84
```

Table 1: Parameters in the output of the **show ip igmp groups** command

Parameter	Description
`Group Address`	Address of the multicast group.
`Interface`	Port through which the group is reachable.

Table 1: Parameters in the output of the **show ip igmp groups** command (cont.)

Parameter	Description
`Uptime`	The time in weeks, days, hours, minutes, and seconds that this multicast group has been known to the device.
`Expires`	Time (in hours, minutes, and seconds) until the entry expires.
`Last Reporter`	Last host to report being a member of the multicast group.

show ip igmp interface

Overview Use this command to display the state of IGMP, IGMP Proxy service, and IGMP Snooping for a specified VLAN, or all VLANs. IGMP is shown as Active or Disabled in the show output.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax `show ip igmp interface [<interface>]`

Parameter	Description
<interface>	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Examples The following output shows IGMP interface status for **vlan2** (with IGMP Snooping enabled):

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

The following output shows IGMP interface status for **vlan2** (with IGMP Snooping disabled):

```
awplus#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
awplus(config)#interface vlan2
awplus(config-if)#no ip igmp snooping
awplus(config-if)#exit
awplus(config)#exit
awplus#show ip igmp interface vlan2
Interface vlan2 (Index 202)
 IGMP Disabled, Inactive, Version 3 (default)
 IGMP interface has 0 group-record states
 IGMP activity: 0 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 255 seconds
 IGMP max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 Source Address checking is enabled
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally disabled
  Num. query-solicit packets: 57 sent, 0 recvd
 IGMP Snooping is not enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

The following command displays the IGMP interface status and Query Solicitation for **vlan3**:

```
awplus#show ip igmp interface vlan3
Interface vlan3 (Index 203)
 IGMP Enabled, Active, Querier, Version 3 (default)
 Internet address is 192.168.9.1
 IGMP interface has 256 group-record states
 IGMP activity: 51840 joins, 0 leaves
 IGMP robustness variable is 2
 IGMP last member query count is 2
 IGMP query interval is 125 seconds
 IGMP query holdtime is 500 milliseconds
 IGMP querier timeout is 250 seconds
 IGMP max query response time is 1 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 251 seconds
 Strict IGMPv3 ToS checking is disabled on this interface
 IGMP Snooping is globally enabled
 IGMP Snooping query solicitation is globally enabled
  Num. query-solicit packets: 1 sent, 10 recvd
 IGMP Snooping is enabled on this interface
 IGMP Snooping fast-leave is not enabled
 IGMP Snooping querier is not enabled
 IGMP Snooping report suppression is enabled
awplus#
```

NOTE: *Query Solicitation status information is highlighted in* ***bold*** *in the above output.*

Use the ***show ip igmp interface*** *command to validate that Query Solicitation is enabled and to show the number of query-solicit message packets sent and received on a VLAN.*

Related Commands

clear ip igmp

clear ip igmp group

clear ip igmp interface

ip igmp

ip igmp last-member-query-count

ip igmp last-member-query-interval

ip igmp querier-timeout

ip igmp query-holdtime

ip igmp query-interval

ip igmp query-max-response-time

ip igmp robustness-variable

ip igmp snooping

ip igmp snooping fast-leave

ip igmp snooping querier

ip igmp snooping report-suppression

ip igmp snooping tcn query solicit

ip igmp version

show ip igmp proxy

Overview Use this command to display the state of IGMP Proxy services for a specified interface or for all interfaces.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip igmp proxy
show ip igmp proxy groups [detail]
show ip igmp proxy groups <multicast-group> [detail]
show ip igmp proxy groups <vlan> [detail]
show ip igmp proxy groups <vlan> <multicast-group> [detail]
```

Parameter	Description
`groups`	Specify IGMP proxy group membership information.
`detail`	Specify detailed IGMPv3 source information.
<vlan>	Specify the name of a single VLAN interface, for example **vlan1**.
<multicast-group>	Specify the IPv4 address in of the multicast group, in the format A.B.C.D.

Mode User Exec and Privileged Exec

Example To display the state of IGMP Proxy services for all interfaces, enter the command:

```
awplus# show ip igmp proxy
```

To display the state of IGMP Proxy services for VLAN interface vlan1, enter the command:

```
awplus# show ip igmp proxy groups vlan1
```

To display the detailed state of IGMP Proxy services for VLAN interface **vlan1**, enter the command:

```
awplus# show ip igmp proxy groups vlan1 detail
```

Related Commands ip igmp proxy-service

show ip igmp snooping mrouter

Overview Use this command to display the multicast router ports, both static and dynamic, in a VLAN.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip igmp snooping mrouter [interface <interface>]
```

Parameter	Description
`interface`	A specific interface.
`<interface>`	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Example To show all multicast router interfaces, use the command:

```
awplus# show ip igmp snooping mrouter
```

To show the multicast router interfaces in `vlan1`, use the command:

```
awplus# show ip igmp snooping mrouter interface vlan1
```

Output Figure 22-3: Example output from the show ip igmp snooping mrouter command

```
VLAN     Interface    Static/Dynamic
1        port1.0.5    Statically configured
200      port1.0.2    Statically configured
```

Figure 22-4: Example output from the show ip igmp snooping mrouter interface vlan1 command

```
VLAN     Interface    Static/Dynamic
1        port1.0.5    Statically configured
```

Related Commands ip igmp snooping mrouter

show ip igmp snooping routermode

Overview Use this command to display the current routermode and the list of IP addresses set as router multicast addresses from the ip igmp snooping routermode command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip igmp snooping routermode
```

Mode User Exec and Privileged Exec

Example To show the routermode and the list of router multicast addresses, use the command:

```
awplus# show ip igmp snooping routermode
```

Output Figure 22-5: Example output from the **show ip igmp snooping router mode** command

```
Router mode.............Def
Reserved multicast address

         224.0.0.1

         224.0.0.2

         224.0.0.4

         224.0.0.5

         224.0.0.6

         224.0.0.9

         224.0.0.13

         224.0.0.15

         224.0.0.24
```

Related Commands ip igmp snooping routermode

show ip igmp snooping statistics

Overview Use this command to display IGMP Snooping statistics data.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip igmp snooping statistics interface <interface-range>
[group [<ip-address>]]
```

Parameter	Description
<ip-address>	Optionally specify the address of the multicast group, entered in the form A.B.C.D.
<interface>	Specify the name of the VLAN interface or interface range.

Mode User Exec and Privileged Exec

Example To display IGMP statistical information for **vlan1** and **vlan2**, use the command:

```
awplus# show ip igmp snooping statistics interface vlan1-vlan2
```

Output Figure 22-6: Example output from the **show ip igmp snooping statistics** command

```
IGMP Snooping statistics for vlan1
Interface:      port1.0.3
Group:          224.1.1.1
Uptime:         00:00:09
Group mode:     Exclude (Expires: 00:04:10)
Last reporter:  10.4.4.5
Source list is empty
IGMP Snooping statistics for vlan2
Interface:      port1.0.4
Group:          224.1.1.2
Uptime:         00:00:19
Group mode:     Exclude (Expires: 00:05:10)
Last reporter:  10.4.4.6
Source list is empty
```

undebug igmp

Overview This command applies the functionality of the no debug igmp command.

23 MLD and MLD Snooping Commands

Introduction

Overview

This chapter provides an alphabetical reference of configuration, clear, and show commands related to MLD and MLD Snooping.

The Multicast Listener Discovery (MLD) module includes the MLD Proxy service and MLD Snooping functionality. Some of the following commands may have commonalities and restrictions; these are described under the Usage section for each command.

NOTE: *MLD and MLD Snooping commands only apply to switch ports, not ETH interfaces.*

IPv6 must be enabled on an interface with the ipv6 enable command, IPv6 forwarding must be enabled globally for routing IPv6 with the ipv6 forwarding command, and IPv6 multicasting must be enabled globally with the ipv6 multicast-routing command before using PIM-SMv6 commands.

The IPv6 Multicast addresses shown can be derived from IPv6 unicast prefixes as per RFC 3306.The IPv6 unicast prefix reserved for documentation is 2001:0db8::/32 as per RFC 3849. Using the base /32 prefix the IPv6 multicast prefix for 2001:0db8::/32 is ff3x:20:2001:0db8::/64. Where an RP address is 2001:0db8::1 the embedded RP multicast prefix is ff7x:120:2001:0db8::/96. For ASM (Any-Source Multicast) the IPV6 multicast addresses allocated for documentation purposes are ff0x::0db8:0:0/96 as per RFC 6676. This is a /96 prefix so that it can be used with group IDs as per RFC 3307. These addresses should not be used for practical networks (other than for testing purposes), nor should they appear in any public network.

The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.

Command List

clear ipv6 mld

Overview Use this command to clear all MLD local memberships on all interfaces.

Syntax
```
clear ipv6 mld
```

Mode Privileged Exec

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Example
```
awplus# clear ipv6 mld
```

Related Commands clear ipv6 mld group

clear ipv6 mld interface

clear ipv6 mld group

Overview Use this command to clear MLD specific local-membership(s) on all interfaces, for a particular group.

Syntax

```
clear ipv6 mld group {*|<ipv6-address>}
```

Parameter	Description
*	Clears all groups on all interfaces. This is an alias to the clear ipv6 mld command.
<ipv6-address>	Specify the group address for which MLD local-memberships are to be cleared from all interfaces. Specify the IPv6 multicast group address in the format in the format X:X::X:X.

Mode Privileged Exec

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Example

```
awplus# clear ipv6 mld group *
```

Related Commands clear ipv6 mld

clear ipv6 mld interface

clear ipv6 mld interface

Overview Use this command to clear MLD interface entries.

Syntax

```
clear ipv6 mld interface <interface>
```

Parameter	Description
<interface>	Specifies name of the interface; all groups learned from this interface are deleted.

Mode Privileged Exec

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Example

```
awplus# clear ipv6 mld interface vlan2
```

Related Commands clear ipv6 mld

clear ipv6 mld group

debug mld

Overview Use this command to enable all MLD debugging modes, or a specific MLD debugging mode.

Use the **no** variant of this command to disable all MLD debugging modes, or a specific MLD debugging mode.

Syntax

```
debug mld {all|decode|encode|events|fsm|tib}
no debug mld {all|decode|encode|events|fsm|tib}
```

Parameter	Description
`all`	Debug all MLD.
`decode`	Debug MLD decoding.
`encode`	Debug MLD encoding.
`events`	Debug MLD events.
`fsm`	Debug MLD Finite State Machine (FSM).
`tib`	Debug MLD Tree Information Base (TIB).

Mode Privileged Exec and Global Configuration

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Examples

```
awplus# configure terminal
awplus(config)# debug mld all
awplus# configure terminal
awplus(config)# debug mld decode
awplus# configure terminal
awplus(config)# debug mld encode
awplus# configure terminal
awplus(config)# debug mld events
```

Output

```
Warning: Console logging enabled
awplus#05:15:00 awplus NSM[1406]: [MLD-DECODE] Dec V2 Grp Rec: Grp ff08::1 on
port2.0.1
05:15:00 awplus NSM[1406]: [MLD-DECODE] Dec V2 Grp Rec: G-Rec not found! on
port2.0.1 for ff08::1
05:15:00 awplus NSM[1406]: [MLD-FSM] Process Event: I=port2.0.1, G=ff08::1, State:
Include, Event: Change To Include
05:15:00 awplus NSM[1406]: [MLD-FSM] State Change: Include(1)->Include(1)
05:15:00 awplus NSM[1406]: [MLD-ENCODE] Send Grp - Src Report: HST-IF vlan1: No
Router Ports found
05:15:00 awplus NSM[1406]: [MLD-DECODE] Socket Read: Ignoring MLD Message on L3
socketsince Snooping is enabled on vlan1
05:15:01 awplus NSM[1406]: [MLD-DECODE] Dec V2 Grp Rec: Grp ff08::1 on port2.0.1
05:15:01 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum
=8511, MsgLen=60
05:15:01 awplus NSM[1406]: [MLD-ENCODE] Send Group - Source Query: Sent G-S Query
on port2.0.1
05:15:01 awplus NSM[1406]: [MLD-FSM] State Change: Include(1)->Exclude(2)
05:15:01 awplus NSM[1406]: [MLD-TIB] Source Rec Del: S=2002::3 Intf=vlan1
05:15:01 awplus NSM[1406]: [MLD-ENCODE] Send Group Report: HST-IF vlan1: No Router
Ports found
05:15:01 awplus NSM[1406]: [MLD-DECODE] Socket Read: Ignoring MLD Message on L3
socketsince Snooping is enabled on vlan1
05:15:01 awplus NSM[1406]: [MLD-EVENTS] Grp - Src Report Rexmit: Exipry for Grp
ff08::1 on vlan1
05:15:01 awplus NSM[1406]: [MLD-EVENTS] Grp - Src Report Rexmit: Group-Source
Report Rexmit failed(-16)
05:15:02 awplus NSM[1406]: [MLD-EVENTS] Grp - Src Query Rexmit: Exipry for Grp
ff08::1 on port2.0.1
05:15:02 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query
Checksum=8511, MsgLen=60
05:15:02 awplus NSM[1406]: [MLD-ENCODE] Send Group - Source Query: Sent G-S Query
on port2.0.1
05:15:02 awplus NSM[1406]: [MLD-EVENTS] Grp Report Rexmit: Exipry for Grp ff08::
1 on vlan1
05:15:02 awplus NSM[1406]: [MLD-ENCODE] Send Group Report: HST-IF vlan1: No Router
Ports found
05:15:02 awplus NSM[1406]: [MLD-EVENTS] Grp - Src Report Rexmit: Exipry for Grp
```

```
ff08::1 on vlan1
05:15:02 awplus NSM[1406]: [MLD-TIB] Source Rec Del: S=2002::3 Intf=vlan1
05:15:03 awplus NSM[1406]: [MLD-EVENTS] Src - Rec Liveness Timer: Exipry for Src
 2002::3 on port2.0.1
005:15:03 awplus NSM[1406]: [MLD-FSM] Process Event: I=port2.0.1, G=ff08::1,
State: Exclude, Event: Source Tmr Expry
05:15:03 awplus NSM[1406]: [MLD-FSM] State Change: Exclude(2)->Exclude(2)
05:15:03 awplus NSM[1406]: [MLD-FSM] Host Process Event: I=vlan1, G=ff08::1,
05:15:06 awplus appmond[1244]: monitoring imi memory usage (max:51200000 kB)
05:15:06 awplus appmond[1244]: monitoring rmond memory usage (max:51200000 kB)
05:15:06 awplus appmond[1244]: monitoring lldpd memory usage (max:51200000 kB)
05:15:06 awplus NSM[1406]: [MLD-EVENTS] Querier Timer: Exipry on port2.0.1, Send
ing General Query 05:15:06 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener
Query Checksum
=14706, MsgLen=28
05:15:06 awplus NSM[1406]: [MLD-ENCODE] Send Gen Query: Sent General Query on
port2.0.1, ret=90
05:15:06 awplus NSM[1406]: [MLD-EVENTS] Querier Timer: Exipry on port2.0.1,
Sending General Query
05:15:06 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum
=14706, MsgLen=28
05:15:06 awplus NSM[1406]: [MLD-ENCODE] Send Gen Query: Sent General Query on
port2.0.1, ret=90
05:15:06 awplus NSM[1406]: [MLD-EVENTS] Querier Timer: Exipry on port2.0.1,
Sending General Query
05:15:06 awplus NSM[1406]: [MLD-ENCODE] MLD Enc Hdr: MLD Listener Query Checksum
=14706, MsgLen=28
05:15:06 awplus NSM[1406]: [MLD-ENCODE] Send Gen Query: Sent General Query on po
rt2.0.1, ret=90
```

Related Commands show debugging mld

ipv6 mld

Overview Use this command to enable the MLD protocol operation on an interface. This command enables MLD protocol operation in stand-alone mode, and can be used to learn local-membership information prior to enabling a multicast routing protocol on the interface.

Use the **no** variant of this command to return all MLD related configuration to the default (including MLD Snooping).

NOTE: *There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.*

There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.

The device has a 512 MLD group limit for (, G) and (S,G) entries.*

Syntax

```
ipv6 mld
no ipv6 mld
```

Default MLD is disabled by default.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld
```

ipv6 mld access-group

Overview Use this command to control the multicast local-membership groups learned on an interface.

Use the **no** variant of this command to disable this access control.

Syntax

```
ipv6 mld access-group <IPv6-access-list-name>
no ipv6 mld access-group
```

Parameter	Description
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Default No access list is configured by default.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Examples In the following example, the VLAN interface `vlan2` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit
ff1e:0db8:0001::/64
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

In the following example, the VLAN interfaces `vlan2-vlan4` will only accept MLD joins for groups in the range `ff1e:0db8:0001::/64`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard group1 permit
ff1e:0db8:0001::/64
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld access-group group1
```

ipv6 mld immediate-leave

Overview Use this command to minimize the leave latency of MLD memberships.

Use the **no** variant of this command to disable this feature.

Syntax

```
ipv6 mld immediate-leave group-list <IPv6-access-list-name>
no ipv6 mld immediate-leave
```

Parameter	Description
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name that defines multicast groups in which the immediate leave feature is enabled. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Default Disabled

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Example The following example shows how to enable the immediate-leave feature on an interface for a specific range of multicast groups. In this example, the router assumes that the group access-list consists of groups that have only one node membership at a time per interface:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld immediate-leave v6grp
awplus(config-if)# exit
```

Related Commands ipv6 mld last-member-query-interval

ipv6 mld last-member-query-count

Overview Use this command to set the last-member query-count value.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ipv6 mld last-member-query-count <value>
no ipv6 mld last-member-query-count
```

Parameter	Description
<value>	Count value. Valid values are from `2 to 7`.

Default The default last-member query-count value is 2.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld last-member-query-count 3
```

ipv6 mld last-member-query-interval

Overview Use this command to configure the interval at which the router sends MLD group-specific host query messages.

Use the **no** variant of this command to set this frequency to the default.

Syntax

```
ipv6 mld last-member-query-interval <milliseconds>
no ipv6 mld last-member-query-interval
```

Parameter	Description
<milliseconds>	The time delay between successive query messages (in milliseconds). Valid values are from 1000 to 25500 milliseconds.

Default 1000 milliseconds

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Example The following example changes the MLD group-specific host query message interval to 2 seconds:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld last-member-query-interval 2000
```

Related Commands ipv6 mld immediate-leave

ipv6 mld limit

Overview Use this command to configure a limit on the maximum number of group memberships that may be learned. The limit may be set for the device as a whole, or for a specific interface.

Once the specified group membership limit is reached, all further local-memberships will be ignored.

Optionally, an exception access-list can be configured to specify the group-address(es) that are exempted from being subject to the limit.

Use the **no** variant of this command to unset the limit and any specified exception access-list.

Syntax

```
ipv6 mld limit <limitvalue> [except <IPv6-access-list-name>]
no ipv6 mld limit
```

Parameter	Description
<limitvalue>	<2-512> Maximum number of group membership states.
<IPv6-access-list-name>	Specify a Standard or an Extended software IPv6 access-list name that defines multicast groups, which are exempted from being subject to the configured limit. See IPv6 Software Access Control List (ACL) Commands for supported IPv6 ACLs.

Default The default limit, which is reset by the **no** variant of this command, is the same as maximum number of group membership entries that can be learned with the **ipv6 mld limit** command.

The default limit of group membership entries that can be learned is 512 entries.

Mode Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols and learned by MLD Snooping.

Examples The following example configures an MLD limit of 100 group-memberships across all VLAN interfaces on which MLD is enabled, and excludes groups in the range `ff1e:0db8:0001::/64` from this limitation:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# ipv6 access-list standard v6grp permit
ff1e:0db8:0001::/64
awplus(config)# ipv6 mld limit 100 except v6grp
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

The following example configures an MLD limit of 100 group-membership states on the VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld limit 100
```

ipv6 mld querier-timeout

Overview Use this command to configure the timeout period before the router takes over as the querier for the interface after the previous querier has stopped querying.

Use the **no** variant of this command to restore the default.

Syntax

```
ipv6 mld querier-timeout <seconds>
no ipv6 mld querier-timeout
```

Parameter	Description
<seconds>	Number of seconds that the router waits after the previous querier has stopped querying before it takes over as the querier. Valid values are from `2 to 65535 seconds`.

Default 255 seconds

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example The following example configures the router to wait 120 seconds from the time it received the last query before it takes over as the querier for the interface:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld querier-timeout 120
```

Related Commands ipv6 mld query-interval

ipv6 mld query-interval

Overview Use this command to configure the frequency of sending MLD host query messages.

Use the **no** variant of this command to return to the default frequency.

Syntax

```
ipv6 mld query-interval <seconds>
no ipv6 mld query-interval
```

Parameter	Description
<seconds>	Variable that specifies the time delay between successive MLD host query messages (in seconds). Valid values are from `1 to 18000 seconds`.

Default The default query interval is 125 seconds.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example The following example changes the frequency of sending MLD host-query messages to 2 minutes:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld query-interval 120
```

Related Commands ipv6 mld querier-timeout

ipv6 mld query-max-response-time

Overview Use this command to configure the maximum response time advertised in MLD queries.

Use the **no** variant of with this command to restore the default.

Syntax

```
ipv6 mld query-max-response-time <seconds>
no ipv6 mld query-max-response-time
```

Parameter	Description
<seconds>	Maximum response time (in seconds) advertised in MLD queries. Valid values are from 1 to 240 seconds.

Default 10 seconds

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example The following example configures a maximum response time of 8 seconds:

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld query-max-response-time 8
```

ipv6 mld robustness-variable

Overview Use this command to change the robustness variable value on an interface.

Use the **no** variant of this command to return to the default on an interface.

Syntax

```
ipv6 mld robustness-variable <value>
no ipv6 mld robustness-variable
```

Parameter	Description
<value>	Valid values are from `1 to 7`.

Default The default robustness variable value is 2.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld robustness-variable 3
```

ipv6 mld snooping

Overview Use this command to enable MLD Snooping. When this command is issued in the Global Configuration mode, MLD Snooping is enabled globally for the device. When this command is issued in Interface mode for a VLAN then MLD Snooping is enabled for the specified VLAN. Note that MLD Snooping is enabled on the VLAN only if it is enabled globally and on the VLAN.

Use the **no** variant of this command to globally disable MLD Snooping in Global Configuration mode, or for the specified VLAN interface in Interface mode.

NOTE: *There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.*

There is a 100 MLD interface limit when applying MLD commands to multiple VLANs. Only the first 100 VLANs have the required multicast structures added to the interfaces that allow multicast routing.

The device has a 512 MLD group limit for (, G) and (S,G) entries.*

Syntax

```
ipv6 mld snooping
no ipv6 mld snooping
```

Default By default, MLD Snooping is enabled both globally and on all VLANs.

Mode Global Configuration and Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage For MLD Snooping to operate on particular VLAN interfaces, it must be enabled both globally by using this command in Global Configuration mode, and on individual VLAN interfaces by using this command in Interface Configuration mode (both are enabled by default).

MLD requires memory for storing data structures, as well as the hardware tables to implement hardware routing. As the number of ports, VLANs, static and dynamic groups increases then more memory is consumed. You can track the memory used for MLD with the command:

```
awplus# show memory pools nsm | grep MLD
```

Static and dynamic groups (LACP), ports and VLANs are not limited for MLD. For VLANs, this allows you to configure MLD across more VLANs with fewer ports per VLAN, or fewer VLANs with more ports per VLAN. For LACPs, you can configure MLD across more LACP groups with fewer ports per LACP, or fewer LACP groups with more ports per LACP.

Examples To configure MLD Snooping on the VLAN interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping
```

To configure MLD Snooping on the VLAN interfaces `vlan2-vlan4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interface `vlan2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config)# no ipv6 mld snooping
```

To disable MLD Snooping for the VLAN interfaces `vlan2-vlan4`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config)# no ipv6 mld snooping
```

To configure MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 mld snooping
```

To disable MLD Snooping globally for the device, enter the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 mld snooping
```

ipv6 mld snooping fast-leave

Overview Use this command to enable MLD Snooping fast-leave processing. Fast-leave processing is analogous to immediate-leave processing; the MLD group-membership is removed as soon as an MLD leave group message is received, without sending out a group-specific query.

Use the **no** variant of this command to disable fast-leave processing.

Syntax

```
ipv6 mld snooping fast-leave
no ipv6 mld snooping fast-leave
```

Default MLD Snooping fast-leave processing is disabled.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command can only be configured on VLAN interfaces.

Examples This example shows how to enable fast-leave processing on the VLAN interface `vlan2`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping fast-leave
```

This example shows how to enable fast-leave processing on the VLAN interface `vlan2- vlan4`.

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping fast-leave
```

ipv6 mld snooping mrouter

Overview Use this command to statically configure the specified port as a Multicast Router interface for MLD Snooping within the specified VLAN.

See detailed usage notes below to configure static multicast router ports when using static IPv6 multicast routes with EPSR, and the destination VLAN is an EPSR data VLAN.

Use the **no** variant of this command to remove the static configuration of the interface as a Multicast Router interface.

Syntax

```
ipv6 mld snooping mrouter interface <port>
no ipv6 mld snooping mrouter interface <port>
```

Parameter	Description
<port>	Specify the name of the port.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command statically configures a switch port as a Multicast Router interface.

Note that if static IPv6 multicast routing is being used with EPSR and the destination VLAN is an EPSR data VLAN, then multicast router (mrouter) ports must be statically configured. This minimizes disruption for multicast traffic in the event of ring failure or restoration.

When configuring the EPSR data VLAN, statically configure mrouter ports so that the multicast router can be reached in either direction around the EPSR ring.

For example, if port1.0.1 and port1.0.6 are ports on an EPSR data VLAN vlan101, which is the destination for a static IPv6 multicast route, then configure both ports as multicast router (mrouter) ports as shown in the example commands listed below:

Output Figure 23-1: Example **ipv6 mld snooping mrouter** commands when static IPv6 multicast routing is being used and the destination VLAN is an EPSR data VLAN:

```
awplus>enable

awplus#configure terminal

awplus(config)#interface vlan101

awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.1

awplus(config-if)#ipv6 mld snooping mrouter interface port1.0.6
```

Examples

This example shows how to specify the next-hop interface to the multicast router for VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

This example shows how to specify the next-hop interface to the multicast router for VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping mrouter interface
port1.0.5
```

Related Commands

ipv6 multicast route

ipv6 mld snooping querier

Overview Use this command to enable MLD querier operation on a subnet (VLAN) when no multicast routing protocol is configured in the subnet (VLAN). When enabled, the MLD Snooping querier sends out periodic MLD queries for all interfaces on that VLAN.

Use the **no** variant of this command to disable MLD querier configuration.

Syntax

```
ipv6 mld snooping querier
no ipv6 mld snooping querier
```

Mode Interface Configuration for a specified VLAN interface.

Usage This command can only be configured on a single VLAN interface - not on multiple VLANs.

The MLD Snooping querier uses the 0.0.0.0 Source IP address because it only masquerades as an MLD querier for faster network convergence.

The MLD Snooping querier does not start, or automatically cease, the MLD Querier operation if it detects query message(s) from a multicast router. It restarts as an MLD Snooping querier if no queries are seen within the other querier interval.

Do not enable MLD Snooping querier if you have already enabled MLD on your device.

Do not enable MLD Snooping querier on your device and then enable MLD afterwards.

Example

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping querier
```

ipv6 mld snooping report-suppression

Overview Use this command to enable report suppression from hosts for Multicast Listener Discovery version 1 (MLDv1) on a VLAN in Interface Configuration mode.

Use the **no** variant of this command to disable report suppression on a VLAN in Interface Configuration mode.

Syntax

```
ipv6 mld snooping report-suppression
no ipv6 mld snooping report-suppression
```

Default Report suppression does not apply to MLDv2, and is turned on by default for MLDv1 reports.

Mode Interface Configuration for a specified VLAN interface or a range of VLAN interfaces.

Usage This MLD Snooping command can only be configured on VLAN interfaces.

MLDv1 Snooping maybe configured to suppress reports from hosts. When a querier sends a query, only the first report for particular set of group(s) from a host will be forwarded to the querier by the MLD Snooping device. Similar reports (to the same set of groups) from other hosts, which would not change group memberships in the querier, will be suppressed by the MLD Snooping device to prevent 'flooding' of query responses.

Examples This example shows how to enable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interface `vlan2`:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 mld snooping report-suppression
```

This example shows how to enable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ipv6 mld snooping report-suppression
```

This example shows how to disable report suppression for MLD reports on VLAN interfaces `vlan2-vlan4`:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ipv6 mld snooping report-suppression
```

ipv6 mld static-group

Overview Use this command to statically configure IPv6 group membership entries on an interface. To statically add only a group membership, do not specify any parameters.

Use the **no** variant of this command to delete static group membership entries.

Syntax

```
ipv6 mld static-group <ipv6-group-address> [source
<ipv6-source-address>] [interface <port>]
```

```
no ipv6 mld static-group <ipv6-group-address> [source
<ipv6-source-address>] [interface <port>]
```

Parameter	Description
<ipv6-group-address>	Specify a standard IPv6 Multicast group address to be configured as a static group member. The IPv6 address uses the format X:X::X:X.
<ipv6-source-address>	Optional. Specify a standard IPv6 source address to be configured as a static source from where multicast packets originate. The IPv6 address uses the format X:X::X:X.
<port>	Optional. Physical interface. This parameter specifies a physical port. If this parameter is used, the static configuration is applied to just to that physical interface. If this parameter is not used, the static configuration is applied on all ports in the VLAN.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to MLD Snooping on a VLAN interface to statically add groups and/or source records.

Examples To add a static group record, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10
```

To add a static group and source record, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 source
fe80::2fd:6cff:fe1c:b
```

To add a static group record on a specific port on vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 mld static-group ff1e::10 interface
port1.0.4
```

ipv6 mld version

Overview Use this command to set the current MLD protocol version on an interface.

Use the **no** variant of this command to return to the default version on an interface.

Syntax

```
ipv6 mld version <version>
no ipv6 mld version
```

Parameter	Description
<version>	MLD protocol version number. Valid version numbers are 1 and 2

Default The default MLD protocol version number is 2.

Mode Interface Configuration for a VLAN interface.

Usage This command applies to interfaces configured for MLD Layer-3 multicast protocols, MLD Snooping. Note this command is intended for use where there is another querier (when there is another device with MLD enabled) on the same link that can only operate with MLD version 1. Otherwise, the default MLD version 2 is recommended for performance.

Example

```
awplus# configure terminal
awplus(config)# ipv6 forwarding
awplus(config)# ipv6 multicast-routing
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 mld version 1
```

show debugging mld

Overview Use this command to display the MLD debugging modes enabled with the debug mld command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging mld
```

Mode Privileged Exec

Example

```
awplus# show debugging mld
```

Output

```
show debugging mld
MLD Debugging status:
  MLD Decoder debugging is on
  MLD Encoder debugging is on
  MLD Events debugging is on
  MLD FSM debugging is on
  MLD Tree-Info-Base (TIB) debugging is on
```

Related Commands debug mld

show ipv6 mld groups

Overview Use this command to display the multicast groups that have receivers directly connected to the router and learned through MLD.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 mld groups [<ipv6-address>|<interface>] [detail]
```

Parameter	Description
<ipv6-address>	Optional. Specify Address of the multicast group in format X:X::X:X.
<interface>	Optional. Specify the Interface name for which to display local information.

Mode User Exec and Privileged Exec

Examples The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups
```

Output Figure 23-2: Example output for **show ipv6 mld groups**

```
awplus#show ipv6 mld groups
MLD Connected Group Membership
Group Address                           Interface            Uptime   Expires
                  Last Reporter
ff08::1                                 vlan10 (port1.0.1)   00:07:27 00:03:10
                  fe80::200:1ff:fe20:b5ac
```

The following command displays local-membership information for all interfaces:

```
awplus# show ipv6 mld groups detail
```

show ipv6 mld interface

Overview Use this command to display the state of MLD and MLD Snooping for a specified interface, or all interfaces.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 mld interface [<interface>]
```

Parameter	Description
<interface>	Interface name.

Mode User Exec and Privileged Exec

Example The following command displays MLD interface status on all interfaces enabled for MLD:

```
awplus# show ipv6 mld interface
```

Output

```
awplus#show ipv6 mld interface

Interface vlan1 (Index 301)
 MLD Enabled, Active, Querier, Version 2 (default)
 Internet address is fe80::215:77ff:fec9:7468
 MLD interface has 0 group-record states
 MLD activity: 0 joins, 0 leaves
 MLD robustness variable is 2
 MLD last member query count is 2
 MLD query interval is 125 seconds
 MLD querier timeout is 255 seconds
 MLD max query response time is 10 seconds
 Last member query response interval is 1000 milliseconds
 Group Membership interval is 260 seconds
 MLD Snooping is globally enabled
 MLD Snooping is enabled on this interface
 MLD Snooping fast-leave is not enabled
 MLD Snooping querier is enabled
 MLD Snooping report suppression is enabled
```

show ipv6 mld snooping mrouter

Overview Use this command to display the multicast router interfaces, both configured and learned, in a VLAN. If you do not specify a VLAN interface then all the VLAN interfaces are displayed.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 mld snooping mrouter [<interface>]
```

Parameter	Description
<interface>	Optional. Specify the name of the VLAN interface. Note: If you do not specify a single VLAN interface, then all VLAN interfaces are shown.

Mode User Exec and Privileged Exec

Examples The following command displays the multicast router interfaces in `vlan2`:

```
awplus# show ipv6 mld snooping mrouter vlan2
```

Output

```
awplus#show ipv6 mld snooping mrouter vlan2
VLAN    Interface    Static/Dynamic
2       port1.0.2    Dynamically Learned
2       port1.0.3    Dynamically Learned
```

The following command displays the multicast router interfaces for all VLAN interfaces:

```
awplus# show ipv6 mld snooping mrouter
```

Output

```
awplus#show ipv6 mld snooping mrouter
VLAN    Interface    Static/Dynamic
2       port1.0.2    Dynamically Learned
2       port1.0.3    Dynamically Learned
3       port1.0.4    Statically Assigned
3       port1.0.5    Statically Assigned
```

show ipv6 mld snooping statistics

Overview Use this command to display MLD Snooping statistics data.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 mld snooping statistics interface <interface>
```

Parameter	Description
<interface>	The name of the VLAN interface.

Mode User Exec and Privileged Exec

Example The following command displays MLDv2 statistical information for `vlan1`:

```
awplus# show ipv6 mld snooping statistics interface vlan1
```

Output

```
awplus#show ipv6 mld snooping statistics interface vlan1
MLD Snooping statistics for vlan1
Interface:      port1.0.1
Group:          ff08::1
Uptime:         00:02:18
Group mode:     Include ()
Last reporter:  fe80::eecd:6dff:fe6b:4783
Group source list: (R - Remote, M - SSM Mapping, S - Static )
  Source Address       Uptime    v2 Exp    Fwd  Flags
  2001:db8::1          00:02:18  00:02:02  Yes  R
  2001:db8::3          00:02:18  00:02:02  Yes  R
```

Part 5: Access and Security

24 IPv4 Hardware Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference of IPv4 Hardware Access Control List (ACL) commands. It contains detailed command information and command examples about IPv4 hardware ACLs, which are applied directly to interfaces using the access-group command

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself.

- Text in parenthesis in command names indicates usage not keyword entry. For example, **access-list hardware (named)** indicates named IPv4 hardware ACLs entered as `access-list hardware` <name> where <*name*> is a placeholder not a keyword.
- Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(access-list standard numbered filter)** represents command entry in the format shown in the syntax `[`<*sequence-number*>`] {deny|permit} {`<source>`|host` <*host-address*>`|any}`.
- Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 24-1: IPv4 Hardware Access List Commands and Prompts

Command Name	Command Mode	Prompt
show interface access-group	Privileged Exec	`awplus#`
show access-list (IPv4 Hardware ACLs)	Privileged Exec	`awplus#`
show interface access-group	Privileged Exec	`awplus#`

Table 24-1: IPv4 Hardware Access List Commands and Prompts (cont.)

Command Name	Command Mode	Prompt
access-group	Global Configuration	`awplus(config)#`
access-list (hardware IP numbered)	Global Configuration	`awplus(config)#`
access-list (hardware MAC numbered)	Global Configuration	`awplus(config)#`
access-list hardware (named)	Global Configuration	`awplus(config)#`
access-group	Interface Configuration	`awplus(config-if)#`
(access-list hardware ICMP filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
(access-list hardware IP protocol filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
(access-list hardware MAC filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
(access-list hardware TCP UDP filter)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`
commit (IPv4)	IPv4 Hardware ACL Configuration	`awplus(config-ip-hw-acl)#`

References

For descriptions of ACLs, and further information about rules when applying them, see the ACL Feature Overview and Configuration Guide.

For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview and Configuration Guide.
- Link Aggregation Commands

Command List

access-group

Overview This command adds or removes a hardware-based access-list to or from a switch port interface. The number of hardware numbered and named access-lists that can be added to a switch port interface is determined by the available memory in hardware-based packet classification tables.

This command works in Interface Configuration mode to apply hardware access-lists to selected switch port interfaces.

The **no** variant of this command removes the selected access-list from an interface.

Syntax

```
access-group
[<3000-3699>|<4000-4699>|<hardware-access-list-name>]
```

```
no access-group
[<3000-3699>|4000-4699|<hardware-access-list-name>]
```

Parameter	Description
<3000-3699>	Hardware IP access-list.
<4000-4699>	Hardware MAC access-list.
<hardware-access-list-name>	The hardware access-list name.

Mode Interface Configuration for a switch port interface

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create an IP access-list that applies the appropriate permit/deny requirements with the access-list (hardware IP numbered) command, the access-list (hardware MAC numbered) command or the access-list hardware (named) command. Then use this command to apply this hardware access- list to a specific port or port range. Note that this command will apply the access-list only to incoming data packets.

To apply ACLs to an LACP aggregated link, apply it to all the individual switch ports in the aggregated group. To apply ACLs to a static channel group, apply it to the static channel group itself. An ACL can even be applied to a static aggregated link that spans more than one switch instance (Link Aggregation Commands).

Note that you cannot apply software numbered ACLs to switch port interfaces with the access-group command. This command will only apply hardware ACLs.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples

To add the numbered hardware access-list `3005` to switch port interface `port1.0.1`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# access-group 3005
```

To add the named hardware access-list `hw-acl` to switch port interface `port1.0.2`, enter the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# access-group hw-acl
```

To apply an ACL to static channel group 2 containing switch `port1.0.5` and `port1.0.6`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.5-1.0.6
awplus(config-if)# static-channel-group 2
awplus(config)# interface sa2
awplus(config-if)# access-group 3000
```

Related Commands

access-list hardware (named)

access-list (hardware IP numbered)

access-list (hardware MAC numbered)

show interface access-group

access-list (hardware IP numbered)

Overview This command creates an access-list for use with hardware classification, such as QoS. The access-list will match on either TCP or UDP type packets that have the specified source and destination IP addresses and Layer 4 port values or ranges. The parameter **any** may be specified if an address does not matter and the port values are optional.

The **no** variant of this command removes the previously specified IP hardware access-list.

Syntax [ip]

```
access-list <3000-3699>
{deny|permit|copy-to-cpu|copy-to-mirror|send-to-mirror|
send-to-cpu} ip <source> <destination> [vlan
<1-4094>]
```

Syntax [icmp]

```
access-list <3000-3699>
{deny|permit|copy-to-cpu|copy-to-mirror|send-to-mirror|
send-to-cpu} icmp <source> <destination>
[icmp-type <type-number>]
```

```
no access-list <3000-3699>
```

Table 25: Parameters in the **access-list (hardware IP numbered)** command - ip|icmp

Parameter	Description
<3000-3699>	Hardware IP access-list number.
deny	Access-list rejects packets that match the source and destination filtering specified with this command.
permit	Access-list permits packets that match the source and destination filtering specified with this command.
copy-to-cpu	Specify packets to copy to the CPU.
copy-to-mirror	Specify packets to copy to the mirror port.
send-to-mirror	Specify packets to send to the mirror port.
send-to-cpu	Specify packets to send to the CPU.
icmp	ICMP packet.
ip	IP packet.

Table 25: Parameters in the **access-list (hardware IP numbered)** command - ip|icmp (cont.)

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host` *<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`icmp-type`	Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.	

Table 25: Parameters in the **access-list (hardware IP numbered)** command - ip|icmp (cont.)

Parameter	Description	
<type-number>	The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.

Syntax [tcp|udp]

```
access-list <3000-3699>
{copy-to-cpu|copy-to-mirror|send-to-mirror|deny|permit|send-to
-cpu} {tcp|udp} <source> {eq <sourceport>|lt
<sourceport>|gt
<sourceport>|ne
<sourceport>|
[range <start-range> <end-range>} <destination> [eq
<destport>|lt <destport>|gt <destport>|ne <destport>]|[range
<start-range> <end-range>]

no access-list <3000-3699>
```

Table 26: Parameters in the **access-list (hardware IP numbered)** command - tcp|udp

Parameter	Description
<3000-3699>	Hardware IP access-list.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`send-to-mirror`	Specify packets to send to the mirror port.
`deny`	The access-list rejects packets that match the type, source, and destination filtering specified with this command.

Table 26: Parameters in the **access-list (hardware IP numbered)** command - tcp|udp (cont.)

Parameter	Description	
`permit`	The access-list permits packets that match the type, source, and destination filtering specified with this command.	
`send-to-cpu`	Specify packets to send to the CPU.	
`tcp`	The access-list matches only TCP packets.	
`udp`	The access-list matches only UDP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 26: Parameters in the **access-list (hardware IP numbered)** command - tcp|udp (cont.)

Parameter	Description
<sourceport>	The source (TCP or UDP) port number, specified as an integer between 0 and 65535.
range	Range of port numbers.
<start-range>	Port number at start of range *<0-65535>*.
<end-range>	Port number at end of range *<0-65535>*.
<destport>	The destination (TCP or UDP) port number, specified as an integer between 0 and 65535.
eq	Matches port numbers that are equal to the port number specified immediately after this parameter.
lt	Matches port numbers that are less than the port number specified immediately after this parameter.
gt	Matches port numbers that are greater than the port number specified immediately after this parameter.
ne	Matches port numbers that are not equal to the port number specified immediately after this parameter.

Syntax [proto]

```
access-list <3000-3699>
{copy-to-cpu|copy-to-mirror|send-to-mirror|deny|permit|send-to
-cpu} proto <ip-protocol> <source> <destination>

no access-list <3000-3699>
```

Table 27: Parameters in the **access-list (hardware IP numbered)** command - proto

Parameter	Description
<3000-3699>	Hardware IP access-list.
copy-to-cpu	Specify packets to copy to the CPU.
copy-to-mirror	Specify packets to copy to the mirror port.
send-to-mirror	Specify packets to send to the mirror port
deny	Access-list rejects packets that match the source and destination filtering specified with this command.
permit	Access-list permits packets that match the source and destination filtering specified with this command.
send-to-cpu	Specify packets to send to the CPU.

Table 27: Parameters in the **access-list (hardware IP numbered)** command - proto (cont.)

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/`*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`proto` *<ip-protocol>*	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	

Table 24-1: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828

Table 24-1: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage This command creates an access-list for use with hardware classification, such as when applying QoS. This command can be used to match ICMP packets, IP protocols, or TCP/ UDP packets.

For ICMP packets, the <3000-3699> range IP hardware access-list will match any ICMP packet that has the specified source and destination IP addresses and ICMP type.

You may apply the **any** parameter if the source or destination IP address is not important. The ICMP type is an optional parameter.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples Follow the below example commands to configure access-lists for ICMP, IP protocol and TCP.

ICMP Example To create an access-list that will permit ICMP packets with a source address of `192.168.1.0/24` with any destination address and an ICMP type of `5` enter the below commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To destroy the access-list with an access-list identity of `3000` enter the below commands:

```
awplus# configure terminal
awplus(config)# no access-list 3000
```

IP Example To create an access-list that will permit any type of IP packet with a source address of `192.168.1.1` and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit ip 192.168.1.1/32 any
```

To create an access-list that will deny all IGMP packets (IP protocol 2) from the 192.168.0.0 network, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 deny proto 2 192.168.0.0/16 any
```

TCP Example

To create an access-list that will permit TCP packets with a destination address of 192.168.1.1, a destination port of 80 and any source address and source port, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 permit tcp any 192.168.1.1/32 eq 80
```

copy-to-mirror Example

To create an access-list that will copy-to-mirror TCP packets with a destination address of 192.168.1.1, a destination port of 80 and any source address and source port for use with the mirror interface command, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 3000 copy-to-mirror tcp any 192.168.1.1/32 eq 80
```

Related Commands

access-group

mirror interface

show running-config

show access-list (IPv4 Hardware ACLs)

access-list (hardware MAC numbered)

Overview This command creates an access-list for use with hardware classification, such as QOS. The access-list will match on packets that have the specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter.

Optionally, the **vlan** and **inner-vlan** parameters can be matched for tagged (802.1q) packets.

The **no** variant of this command removes the specified MAC hardware filter access-list.

Syntax

```
access-list <4000-4699>
{copy-to-cpu|copy-to-mirror|deny|permit|send-to-cpu}
{<source-mac-address> <source-mac-mask>|any}
{<destination-mac-address> <destination-mac-mask>|any}
[vlan <1-4094> [inner-vlan <1-4094>]]

no access-list <4000-4699>
```

Parameter	Description
<4000-4699>	Hardware MAC access-list.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`deny`	Access-list rejects packets that match the source and destination filtering.
`permit`	Access-list permits packets that match the source and destination filtering.
`send-to-cpu`	Specify packets to send to the CPU.
<source-mac-address>	The source MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each *H* is a hexadecimal number that represents a 4 bit binary number.
<source-mac-mask	The mask that will be applied to the source MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each *H* is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any source MAC address.
<destination-mac-address>	The destination MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.

Parameter	Description
<destination-mac-mask>	The mask that will be applied to the destination MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any destination MAC address.
`vlan`	Specifies that the ACL will match on the ID in the packet's VLAN tag.
<1-4094>	The VLAN VID.
`inner-vlan`	This parameter is used within double-tagged VLANs. It is the inner VLAN tag (VID); sometimes referred to as the C-TAG (Customer VLAN TAG), where the vlan VID tag is referred to as the S-TAG (Service VLAN TAG).
<1-4094>	The inner VLAN VID.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage This command creates an access-list for use with hardware classification, such as when applying QoS. The <4000-4699> range MAC hardware access-list will match on packets that have the specified source and destination MAC addresses. You may apply the **any** parameter if the source or destination MAC host address is not important.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To create an access-list that will permit packets with a MAC address of `0000.00ab.1234` and any destination address enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4000 permit 0000.00ab.1234 0000.0000.0000 any
```

To create an access-list that will permit packets with an initial MAC address component of `0000.00ab` and any destination address, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit 0000.00ab.1234 0000.0000.FFFF any
```

To create an access-list that will copy-to-mirror packets with an initial MAC address component of `0000.00ab` and any destination address for use with the mirror interface command, enter the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 copy-to-mirror 0000.00ab.1234 0000.0000.FFFF any
```

To destroy the access-list with an access-list identity of `4000` enter the commands:

```
awplus# configure terminal
awplus(config)# no access-list 4000
```

Related Commands

access-group

mirror interface

show running-config

show access-list (IPv4 Hardware ACLs)

access-list hardware (named)

Overview This command creates a named hardware access-list and puts you into IPv4 Hardware ACL Configuration mode, where you can add filters to the ACL. Once you have configured the ACL, you can apply it to a switch port.

The **no** variant of this command removes the specified named hardware ACL.

Syntax

```
access-list hardware <hardware-access-list-name>
no access-list hardware <hardware-access-list-name>
```

Parameter	Description
<hardware-access-list-name>	Specify the hardware ACL name to then define ACL filters for in the subsequent IPv4 Hardware ACL Configuration mode.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage Use this command to name a hardware ACL and enter the IPv4 Hardware ACL Configuration mode. If the named hardware ACL does not exist, it will be created after entry. If the named hardware ACL does exist, then you can enter IPv4 Hardware ACL Configuration mode for that existing ACL.

Entering this command with the hardware ACL name moves you to the `(config-ip- hw-acl)` prompt for the IPv4 Hardware ACL Configuration mode so you can enter ACL filters with sequence numbers. From this prompt, configure the filters for the ACL. See the ACL Feature Overview and Configuration Guide for complete examples of configured sequenced numbered ACLs.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To create the hardware access-list named `ACL-1` and enter the IPv4 Hardware ACL Configuration mode to specify the ACL filter entry, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware ACL-1
awplus(config-ip-hw-acl)#
```

To remove the hardware access-list named `ACL-1`, use the commands:

```
awplus# configure terminal
awplus(config)# no access-list hardware ACL-1
```

Related Commands

access-group

(access-list hardware ICMP filter)

(access-list hardware IP protocol filter)

(access-list hardware TCP UDP filter)

(access-list standard named filter)

show access-list (IPv4 Hardware ACLs)

(access-list hardware ICMP filter)

Overview

Use this ACL filter to add a new ICMP filter entry to the current hardware access-list. The filter will match on any ICMP packet that has the specified source and destination IP addresses and ICMP type. The parameter **any** may be specified if an address does not matter and the ICMP type is an optional parameter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current hardware access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the command, the show access-list (IPv4 Hardware ACLs) command.

Syntax [icmp]

```
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} icmp
<source> <destination> [icmp <icmp-value>]
```

```
no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} icmp
<source> <destination> [icmp <icmp-value>]
```

```
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.
`send-to-cpu`	Specify packets to send to the CPU.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`icmp`	ICMP packet type.

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	`any`	Matches any source IP address.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	`any`	Matches any destination IP address.
`icmp-type`	The ICMP type.	
<icmp-value>	The value of the ICMP type.	

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the access-group command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *You must reach the prompt awplus(config-ip-hw-acl)# by running the access-list hardware (named) command, and entering an appropriate access-list name.*

*Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples

To add an access-list filter entry with a sequence number of `100` to the access-list named `my-list` that will permit ICMP packets with a source address of `192.168.1.0/24`, any destination address and an icmp type of `5`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 100 permit icmp 192.168.1.0/24 any
icmp-type 5
```

To remove an access-list filter entry with a sequence number of `100`in the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no 100
```

Related Commands

access-list hardware (named)

show running-config

show access-list (IPv4 Hardware ACLs)

(access-list hardware IP protocol filter)

Overview

Use this ACL filter to add an IP protocol type filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination IP addresses and IP protocol type, or has the optionally specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol type filter entry from the current hardware access-list. You can specify the IP protocol type filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP protocol type filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Hardware ACLs) command.

Syntax [any|ip|proto]

```
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
{any|ip|proto <ip-protocol>}
{<source>|dhcpsnooping|any} {<destination>|any}
[mac {<mac-source-address> <mac-source-mask>|any]
{<mac-destination-address> <mac-destination-mask>|any}

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
{any|ip|proto <ip-protocol>}
{<source>|dhcpsnooping} {<destination>|any}
[mac {<mac-source-address> <mac-source-mask>|any]
{<mac-destination-address> <mac-destination-mask>|any}

no <sequence-number>
```

Parameter	Description
`<sequence-number>`	<1-65535> The sequence number for the filter entry of the selected access control list.
`deny`	Access-list rejects packets of the type specified.
`permit`	Access-list allows packets of the type specified
`send to cpu`	Specify packets to send to the CPU.
`copy to cpu`	Specify packets to copy to the CPU.
`copy to mirror`	Specify packets to copy to the mirror port.
`ip`	IP packets.
`any`	Any packet.

Parameter	Description	
`proto <ip-protocol>`	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	
`dhcpsnooping`	The source address learned from the DHCP Snooping binding database.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host<ip-addr>`	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host<ip-addr>`	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> <reverse-mask>	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Parameter	Description
`mac`	Signifies a MAC and based hardware access-list.
<mac-source-address>	The source host's MAC address, entered in HHHH.HHHH.HHHH format.
<mac-source-mask>	The source host's MAC wildcard mask entered in HHHH.HHHH.HHHH format. where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Matches any source MAC address.
<mac-destination-address>	The destination host's MAC address, entered in HHHH.HHHH.HHHH format.
<mac-destination-mask>	The destination host's wildcard mask entered in HHHH.HHHH.HHHH format. where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Matches any destination MAC address.

Table 24-2: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]

Table 24-2: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the access-group command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list hardware (named) command. with the required access control list number, or name, but with no further parameters selected.*

*Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples

To add an access-list filter entry to the access-list named `my-list` that will permit any type of IP packet with a source address of `192.168.1.1` and any destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any
```

To add an access-list filter entry to the access-list named `my-list` that will permit any type of IP packet with a source address of `192.168.1.1`and a MAC source address of `ffee.ddcc.bbaa` with any IP and MAC destination address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit ip 192.168.1.1/32 any mac
ffee.ddcc.bbaa any
```

To add an access-list filter entry to the access-list named `my-list` a filter that will deny all IGMP packets (protocol `2`) from the `192.168.0.0` network with sequence number `50` in access-list, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# 50 deny proto 2 192.168.0.0/16 any
```

Related Commands

access-list hardware (named)

show running-config

show access-list (IPv4 Hardware ACLs)

(access-list hardware MAC filter)

Overview

Use this ACL filter to add a MAC filter entry to the current hardware access-list. The filter will match on any IP packet that has the specified source and destination MAC addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a MAC filter entry from the current hardware access-list. You can specify the MAC filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its MAC filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Hardware ACLs) command.

Syntax [mac]

```
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
mac {<source-mac-address> <source-mac-mask>|any}
{<destination-mac-address> <destination-mac-mask>|any}
[{vlan <1-4094>|inner-vlan <1-4094>}]

no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
mac {<source-mac-address> <source-mac-mask>|any}
{<destination-mac-address> <destination-mac-mask>|any}
[{vlan <1-4094>|inner-vlan <1-4094>}]

no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specify packets to reject.
permit	Specify packets to accept.
send-to-cpu	Specify packets to send to the CPU.
copy-to-cpu	Specify packets to copy to the CPU.
copy-to-mirror	Specify packets to copy to the CPU.
mac	MAC address.
<source-mac-address>	The source MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.

Parameter	Description
<source-mac-mask>	The mask that will be applied to the source MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any source MAC host.
<destination-mac-address>	The destination MAC address of the packets. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number.
<destination-mac-mask>	The mask that will be applied to the destination MAC addresses. Enter this in the format <HHHH.HHHH.HHHH> where each H is a hexadecimal number that represents a 4 bit binary number. For a mask, each value will be either `0` or `F`. Where Hex `FF` = Ignore, and Hex `00` = Match.
`any`	Any destination MAC host.

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the access-group command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number

NOTE: *The access control list being configured is selected by running the access-list hardware (named) command. with the required access control list number, or name, but with no further parameters selected.*

*Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To add an access-list filter entry to the access-list named `my-list` that will permit packets with a source MAC address of `0000.00ab.1234` and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# permit mac 0000.00ab.1234
0000.0000.0000 any
```

To remove an access-list filter entry that permit packets with a source MAC address of `0000.00ab.1234` and any destination MAC address, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-list
awplus(config-ip-hw-acl)# no permit mac 0000.00ab.1234
0000.0000.0000 any
```

Related Commands

access-group

access-list hardware (named)

show running-config

(access-list hardware TCP UDP filter)

Overview

Use this ACL filter to add a TCP or UDP filter entry to the current hardware access-list. The filter will match on any TCP or UDP type packet that has the specified source and destination IP addresses. The parameter **any** may be specified if an address does not matter. If a sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current hardware access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Hardware ACLs) command.

Syntax [tcp|udp]

```
[<sequence-number>]
{deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror} {tcp|udp}
[<source> {eq <sourceport>|gt <sourceport>|lt <sourceport>|
ne <sourceport>|range <start-range> <end-range>}]
[<destination> {eq <destport>|gt <destport>|lt <destport>|
ne <destport>|range <start-range> <end-range>}]
```

```
no {deny|permit|send-to-cpu|copy-to-cpu|copy-to-mirror}
{tcp|udp} [<source>
{eq <sourceport>|gt <sourceport>|lt <sourceport>|
ne <sourceport>|range <start-range> <end-range>}]
[<destination> {eq <destport>|gt <destport>|lt <destport>|
ne <destport>|range <start-range> <end-range>}]
```

```
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Access-list rejects packets that match the source and destination filtering specified with this command.
permit	Access-list permits packets that match the source and destination filtering specified with this command.
send-to-cpu	Specify packets to send to the CPU.
copy-to-cpu	Specify packets to copy to the CPU.
copy-to-mirror	Specify packets to copy to the mirror port.
tcp	TCP packets.
udp	UDP packets.

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<sourceport>	The source TCP or UDP port number, specified as an integer between 0 and 65535.	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`eq`	Equal to.	
`lt`	Less than.	
`gt`	Greater than.	
`ne`	Not equal to.	

Parameter	Description
<destport>	The destination TCP or UDP port number, specified as an integer between 0 and 65535.
range	Specify the range of port numbers between 0 and 65535.
<start-range>	The source or destination port number at the start of the range *<0-65535>*.
<end-range>	The source or destination port number at the end of the range *<0-65535>*.

Mode IPv4 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage First create a named hardware access-list that applies the appropriate permit/deny requirements. Then use the access-group command to apply this access-list to a specific port or range. Note that this command will apply the access-list only to **incoming** data packets.

An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list hardware (named) command. with the required access control list number, or name, but with no further parameters selected.*

*Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Example To add an access-list filter entry to access-list named `my-hw-list` that will permit TCP packets with a destination address of `192.168.1.1`, a destination port of `80`, and any source address, and source port, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# permit tcp any 192.168.1.1/32 eq 80
```

Related Commands access-list hardware (named)

show running-config

show access-list (IPv4 Hardware ACLs)

commit (IPv4)

Overview Use this command to commit the IPv4 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv4 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv4 ACLs to synchronize.

Syntax

```
commit
```

Mode IPv4 Hardware ACL Configuration

Usage Normally, when an IPv4 hardware ACL is edited, the new configuration state of the IPv4 ACL is not written to hardware until you exit IPv4 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the exit command to exit configuration modes, potentially leading to IPv4 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv4 hardware ACL filter ensures that it is updated in the hardware immediately.

Example To update the hardware with the IPv4 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# access-list hardware my-hw-list
awplus(config-ip-hw-acl)# commit
```

Related Commands access-list hardware (named)

show access-list (IPv4 Hardware ACLs)

Overview Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list.

Syntax

```
show access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|<4000-4499>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (standard - expanded range).
<2000-2699>	IP extended access-list (extended - expanded range).
<3000-3699>	Hardware IP access-list.
<4000-4499>	Hardware MAC access-list.
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Examples To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
    deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
    permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
    permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the below error message if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

Related Commands

access-list extended (named)

access-list (hardware MAC numbered)

access-list hardware (named)

show interface access-group

Overview Use this command to display the access groups attached to a port. If an access group is specified, then the output only includes the ports that the specified access group is attached to. If no access group is specified then this command displays all access groups that are attached to the ports that are specified with <port-list>.

Note that **access group** is the term given for an access-list when it is applied to an interface.

NOTE: *This command will function on your switch in stand-alone mode. but is not supported when the device forms part of a VCStack.*

Syntax

```
show interface <port-list> access-group
[<3000-3699>|<4000-4699>]
```

Parameter	Description
<port-list>	Specify the ports to display information. A port-list can be either: • a switch port (e.g. port1.0.6) a static channel group (e.g. sa2) or a dynamic (LACP) channel group (e.g. po2) • a continuous range of ports separated by a hyphen, e.g. port1.0.1-1.0.6 or port1.0.1-port1.0.6 or po1-po2 • a comma-separated list of ports and port ranges, e.g. port1.0.1,port1.0.3-1.0.6. Do not mix switch ports, static channel groups, and LACP channel groups in the same list.
`access group`	Select the access group whose details you want to show.
<3000-3699>	Specifies the Hardware IP access-list.
<4000-4699>	Specifies the Hardware MAC access-list.

Mode User Exec and Privileged Exec

Example To show all access-lists attached to `port1.0.1`, use the command:

```
awplus# show interface port1.0.1 access-group
```

Output Figure 24-1: Example output from the show interface access-group command

```
Interface port1.0.1
  access-group 3000
  access-group 3002
  access-group 3001
```

Related Commands access-group

25 IPv4 Software Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference for the IPv4 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv4 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview_and_Configuration Guide.
- Link Aggregation Commands

NOTE: *Text in parenthesis in command names indicates usage not keyword entry. For example,* ***access-list hardware (named)*** *indicates named IPv4 hardware ACLs entered as* `access-list hardware <name>` *where <name> is a placeholder not a keyword.*

Parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as ***(access-list standard numbered filter)*** *represents command entry in the format shown in the syntax* `[<sequence-number>] {deny|permit} {<source>|host <host-address>|any}`.

Software ACLs will ***deny*** *access unless* ***explicitly permitted*** *by an ACL action.*

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 25-1: IPv4 Software Access List Commands and Prompts

Command Name	Command Mode	Prompt
show ip access-list	Privileged Exec	awplus#
access-group	Global Configuration	awplus(config)#
access-list (extended named)	Global Configuration	awplus(config)#
access-list (extended numbered)	Global Configuration	awplus(config)#
access-list (standard named)	Global Configuration	awplus(config)#
access-list (standard numbered)	Global Configuration	awplus(config)#
maximum-access-list	Global Configuration	awplus(config)#
dos	Interface Configuration	awplus(config-if)#
(access-list extended ICMP filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list extended IPfilter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list extended IP protocol filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list extended TCP UDP filter)	IPv4 Extended ACL Configuration	awplus(config-ip-ext-acl)#
(access-list standard named filter)	IPv4 Standard ACL Configuration	awplus(config-ip-std-acl)#
(access-list standard numbered filter)	IPv4 Standard ACL Configuration	awplus(config-ip-std-acl)#

Command List

access-list extended (named)

Overview

This command configures an extended named access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list name.

The **no** variant of this command removes a specified extended named access-list.

Syntax [list-name]

```
access-list extended <list-name>
no access-list extended <list-name>
```

Parameter	Description
<list-name>	A user-defined name for the access-list

Syntax [icmp]

```
access-list extended <list-name>{deny|permit} icmp <source>
<destination> [icmp-type <type-number>] [log]
no access-list extended <list-name>{deny|permit} icmp <source>
<destination> [icmp-type <type-number>] [log]
```

Table 25-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description
<list-name>	A user-defined name for the access-list.
deny	The access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The access-list permits packets that match the type, source, and destination filtering specified with this command.
icmp	The access-list matches only ICMP packets.
icmp-type	Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.

Table 25-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 25-2: Parameters in the access-list extended (named) command - icmp

Parameter	Description	
<type-number>	The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`log`	Logs the results.	

Syntax [tcp|udp]

```
access-list extended <list-name> {deny|permit} {tcp|udp}
<source> [eq <sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>] <destination> [eq <destport>|lt <destport>|gt
<destport>|ne <destport>] [log]
```

```
no access-list extended <list-name> {deny|permit} {tcp|udp}
<source> [eq <sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>] <destination> [eq <destport> |lt <destport>|gt
<destport>|ne <destport>][log]
```

Table 25-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description
<list-name>	A user-defined name for the access-list.
`deny`	The access-list rejects packets that match the type, source, and destination filtering specified with this command.
`permit`	The access-list permits packets that match the type, source, and destination filtering specified with this command.
`tcp`	The access-list matches only TCP packets.
`udp`	The access-list matches only UDP packets.

Table 25-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/ *<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/ *<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
<sourceport>	The source port number, specified as an integer between 0 and 65535.	
<destport>	The destination port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers greater than the port number specified immediately after this parameter.	

Table 25-3: Parameters in the access-list extended (named) command - tcp|udp

Parameter	Description
`ne`	Matches port numbers not equal to the port number specified immediately after this parameter.
`log`	Log the results.

Syntax [proto|any| ip]

```
access-list extended <list-name> {deny|permit} {proto
<ip-protocol>|any|ip} {<source>} {<destination>} [log]
```

```
no access-list extended <list-name>{deny|permit} {proto
<ip-protocol>|any|ip}{<source>}{<destination>}[log]
```

Table 25-4: Parameters in the access-list extended (named) command - proto|ip|any

Parameter	Description	
<list-name>	A user-defined name for the access-list.	
`deny`	The access-list rejects packets that match the type, source, and destination filtering specified with this command.	
`permit`	The access-list permits packets that match the type, source, and destination filtering specified with this command.	
`proto`	Matches only a specified type of IP Protocol.	
`any`	The access-list matches any type of IP packet.	
`ip`	The access-list matches only IP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>/*<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.

Table 25-4: Parameters in the access-list extended (named) command - proto|ip|any (cont.)

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr>`/` *<prefix>*	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr> *<reverse-mask>*	Alternatively, you can enter a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
`log`	Logs the results.	
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	

Table 25-5: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]

Table 25-5: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring access-lists for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list extended** followed by only the name. Entering only the name moves you to the IPv4 Extended ACL Configuration mode for the selected access-list.

From there you can configure your access-lists by using the commands (access-list extended ICMP filter), (access-list extended IP filter), and (access-list extended IP protocol filter).

Note that packets must match both the source and the destination details.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples You can enter the extended named ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```
awplus# configure terminal
awplus(config)# access-list extended TK deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24 eq 12 log
```

Alternatively, you can enter the extended named ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list extended TK
awplus(config-ip-ext-acl)# deny tcp 2.2.2.3/24 eq 14 3.3.3.4/24 eq 12 log
```

access-list (extended numbered)

Overview

This command configures an extended numbered access-list that permits or denies packets from specific source and destination IP addresses. You can either create an extended numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Extended ACL Configuration mode for sequenced ACL filter entry after entering a list number.

The **no** variant of this command removes a specified extended named access-list.

Syntax [list-number]

```
access-list {<100-199>|<2000-2699>}
no access-list {<100-199>|<2000-2699>}
```

Parameter	Description
<100-199>	IP extended access-list.
<2000-2699>	IP extended access-list (expanded range).

Syntax [deny|permit]

```
access-list {<100-199>|<2000-2699>} {deny|permit} ip <source> <destination>
no access-list {<100-199>|<2000-2699>}{deny|permit} ip <source> <destination>
```

Parameter	Description	
<100-199>	IP extended access-list.	
<2000-2699>	IP extended access-list (expanded range).	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`. This matches any source IP address within the specified subnet.

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	An IPv4 address, followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`. This matches any destination IP address within the specified subnet.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring access-list for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list** followed by only the number. Entering only the number moves you to the IPv4 Extended ACL Configuration mode for the selected access-list. From there you can configure your access-lists by using the commands (access-list extended ICMP filter), (access-list extended IP filter), and (access-list extended IP protocol filter).

Note that packets must match both the source and the destination details.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples You can enter the extended ACL in the Global Configuration mode together with the ACL filter entry on the same line, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101 deny ip 172.16.10.0 0.0.0.255 any
```

Alternatively, you can enter the extended ACL in Global Configuration mode before specifying the ACL filter entry in the IPv4 Extended ACL Configuration mode, as shown below:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# deny ip 172.16.10.0 0.0.0.255 any
```

(access-list extended ICMP filter)

Overview Use this ACL filter to add a new ICMP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an ICMP filter entry from the current extended access-list. You can specify the ICMP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its ICMP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [icmp]

```
[<sequence-number>] {deny|permit} icmp <source> <destination>
[icmp-type <icmp-value>] [log]
```

```
no {deny|permit} icmp <source> <destination>[icmp-type
<icmp-value>] [log]
```

```
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
icmp	ICMP packet type.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	any	Matches any destination IP address.

Parameter	Description
`icmp-type`	The ICMP type.
`<icmp-value>`	The value of the ICMP type.
`log`	Log the results.

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add a new entry in access-list called `my-list` that will reject ICMP packets from `10.0.0.1` to `192.168.1.1`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny icmp 10.0.0.1/32 192.168.1.1/32
```

Use the following commands to add a new filter at sequence number `5` position of the access-list called `my-list`. The filter will accept the ICMP type `8` packets from `10.1.1.0/24` network, to `192.168.1.0` network:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit icmp 10.1.1.0/24
192.168.1.0/24 icmp-type 8
```

(access-list extended IP filter)

Overview Use this ACL filter to add a new IP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [ip]

```
[<sequence-number>] {deny|permit} ip <source> <destination>
no {deny|permit} ip <source> <destination>
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
`deny`	Access-list rejects packets that match the source and destination filtering specified with this command.	
`permit`	Access-list permits packets that match the source and destination filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	`any`	Matches any source IP address.
	`host`*<ip-addr>*	Matches a single source host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter `192.168.1.1 0.0.0.255`.

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	`any`	Matches any destination IP address.
	`host`*<ip-addr>*	Matches a single destination host with the IP address given by *<ip-addr>* in dotted decimal notation.
	<ip-addr> *<reverse-mask>*	Alternatively, enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, enter `192.168.1.1 0.0.0.255`.

Mode Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [list-number] First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a numbered extended access-list `101`:

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the numbered extended access- list `101` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

Example 2 [list-name] First use the following commands to enter the IPv4 Extended ACL Configuration mode and define a named access-list called `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)#
```

Then use the following commands to add a new entry to the named access-list `my-acl` that will reject packets from `10.0.0.1` to `192.168.1.1`:

```
awplus(config-ip-ext-acl)# deny ip host 10.0.0.1 host
192.168.1.1
awplus(config-ip-ext-acl)# 20 permit ip any any
```

Example 3 [list-number] Use the following commands to remove the access-list filter entry with sequence number `20` from extended numbered access-list `101`.

```
awplus# configure terminal
awplus(config)# access-list 101
awplus(config-ip-ext-acl)# no 20
```

Example 4 [list-name] Use the following commands to remove the access-list filter entry with sequence number `20` from extended named access-list `my-acl`:

```
awplus# configure terminal
awplus(config)# access-list extended my-acl
awplus(config-ip-ext-acl)# no 20
```

(access-list extended IP protocol filter)

Overview Use this ACL filter to add a new IP protocol type filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes an IP protocol filter entry from the current extended access-list. You can specify the IP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its IP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [proto]

```
[<sequence-number>] {deny|permit} proto <ip-protocol> <source> <destination> [log]
no {deny|permit} proto <ip-protocol> <source> <destination> [log]
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
proto *<ip-protocol>*	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	`any`	Matches any destination IP address.
`log`	Log the results.	

Table 25-6: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]

Table 25-6: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [creating a list] Use the following commands to add a new access-list filter entry to the access-list named `my-list` that will reject IP packets from source address `10.10.1.1/32` to destination address `192.68.1.1/32`:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny ip 10.10.1.1/32 192.168.1.1/32
```

Example 2 [adding to a list]

Use the following commands to add a new access-list filter entry at sequence position `5` in the access-list named `my-list` that will accept packets from source address `10.10.1.1/24` to destination address `192.68.1.1/24`:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit ip 10.10.1.1/24
192.168.1.1/ 24
```

(access-list extended TCP UDP filter)

Overview

Use this ACL filter to add a new TCP or UDP filter entry to the current extended access-list. If the sequence number is specified, the new filter is inserted at the specified location. Otherwise, the new filter is added at the end of the access-list.

The **no** variant of this command removes a TCP or UDP filter entry from the current extended access-list. You can specify the TCP or UDP filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its TCP or UDP filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit} {tcp|udp} <source> {eq
<sourceport> |lt <sourceport>|gt <sourceport>|ne <sourceport>}
<destination> [eq <destport>|lt <destport>|gt <destport>|ne
<destport>] [log]
```

```
no [<sequence-number>]{deny|permit} {tcp|udp} <source> {eq
<sourceport> |lt <sourceport>|gt <sourceport>|ne <sourceport>}
<destination> [eq <destport>|lt <destport>|gt <destport>|ne
<destport>] [log]
```

```
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets that match the source and destination filtering specified with this command.	
permit	Access-list permits packets that match the source and destination filtering specified with this command.	
tcp	The access-list matches only TCP packets.	
udp	The access-list matches only UDP packets.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.
<sourceport>	The source port number, specified as an integer between 0 and 65535.	

Parameter	Description	
<destination>	The destination address of the packets. You can specify a single host, a subnet, or all destinations. The following are the valid formats for specifying the destination:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	`any`	Matches any destination IP address.
<destport>	The destination port number, specified as an integer between 0 and 65535.	
`eq`	Matches port numbers equal to the port number specified immediately after this parameter.	
`lt`	Matches port numbers less than the port number specified immediately after this parameter.	
`gt`	Matches port numbers greater than the port number specified immediately after this parameter.	
`ne`	Matches port numbers not equal to the port number specified immediately after this parameter.	
`log`	Log the results.	

Mode IPv4 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (extended numbered) command or the access-list extended (named) command, with the required access control list number, or name - but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [creating a list] To add a new entry to the access-list named `my-list` that will reject TCP packets from `10.0.0.1`on TCP port `10` to `192.168.1.1` on TCP port `20`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# deny tcp 10.0.0.1/32 eq 10
192.168.1.1/32 eq 20
```

Example 2 [adding to a list]

To insert a new entry with sequence number `5` of the access-list named `my-list` that will accept UDP packets from `10.1.1.0/24` network to `192.168.1.0/24` network on UDP port `80`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list extended my-list
awplus(config-ip-ext-acl)# 5 permit udp 10.1.1.0/24
192.168.1.0/24 eq 80
```

access-list standard (named)

Overview This command configures a standard named access-list that permits or denies packets from a specific source IP address. You can either create a standard named ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list name.

The **no** variant of this command removes a specified standard named access-list.

Syntax [list-name]

```
access-list standard <standard-access-list-name>
no access-list standard <standard-access-list-name>
```

Parameter	Description
<standard-access-list-name>	Specify a name for the standard access-list.

Syntax [deny|permit]

```
access-list standard <standard-access-list-name> {deny|permit} <source>
no access-list standard <standard-access-list-name> {deny|permit} <source>
```

Parameter	Description	
<standard-access-list-name>	Specify a name for the standard access-list.	
deny	The access-list rejects packets that match the source filtering specified with this command.	
permit	The access-list permits packets that match the source filtering specified with this command.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any source IP address within the specified subnet.
	any	Matches any source IP address.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring a standard named access-list for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list standard** followed by only the name. Entering only the name moves you to the IPv4 Standard ACL Configuration mode for the selected access-list. From there you can configure your access-lists by using the command (access-list standard named filter).

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To define a standard access-list named `my-list` and deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list deny any
```

Alternatively, to define a standard access-list named `my-list` and enter the IPv4 Standard ACL Configuration mode to deny any packets from any source, use the commands:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 5 deny any
```

Related Commands (access-list standard named filter)

show running-config

show ip access-list

access-list (standard numbered)

Overview This command configures a standard numbered access-list that permits or denies packets from a specific source IP address. You can either create a standard numbered ACL together with an ACL filter entry in the Global Configuration mode, or you can use the IPv4 Standard ACL Configuration mode for sequenced ACL filter entry after first entering an access-list number.

The **no** variant of this command removes a specified standard numbered access-list.

Syntax [list-number]

```
access-list {<1-99>|<1300-1999>}
no access-list {<1-99>|<1300-1999>}
```

Parameter	Description
<1-99>	IP standard access-list.
<1300-1999>	IP standard access-list (expanded range).

Syntax [deny|permit]

```
access-list {<1-99>|<1300-1999>} {deny|permit} <source>
no access-list {<1-99>|<1300-1999>} {deny|permit} <source>
```

Parameter	Description	
<1-99>	IP standard access-list.	
<1300-1999>	IP standard access-list (expanded range).	
`deny`	Access-list rejects packets from the specified source.	
`permit`	Access-list accepts packets from the specified source.	
<source>	The source address of the packets. You can specify a single host, a subnet, or all sources. The following are the valid formats for specifying the source:	
	<ip-addr> <reverse-mask>	Enter an IPv4 address followed by a reverse mask in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	`any`	Matches any source IP address.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use this command when configuring a standard numbered access-list for filtering IP software packets.

You can either create access-lists from within this command, or you can enter **access-list** followed by only the number. Entering only the number moves you to the IPv4 Standard ACL Configuration mode for the selected access-list. From there you can configure your access-lists by using the command (access-list standard numbered filter).

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples

To create ACL number `67` that will deny packets from subnet `172.16.10`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67 deny 172.16.10.0 0.0.0.255
```

Alternatively, to enter the IPv4 Standard ACL Configuration mode to create the ACL filter and deny packets from subnet `172.16.10.0` for the standard numbered access-list `67`, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 67
awplus(config-ip-std-acl)# deny 172.16.10.0 0.0.0.255
```

Related Commands

(access-list standard named filter)

show running-config

show ip access-list

(access-list standard named filter)

Overview This ACL filter adds a source IP address filter entry to a current named standard access-list. If the sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current named standard access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax

```
[<sequence-number>] {deny|permit} {<source> [exact-match]|any}
no {deny|permit} {<source> [exact-match]|any}
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets of the source filtering specified.	
permit	Access-list allows packets of the source filtering specified	
<source>	The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:	
	<ip-addr>/<prefix>	An IPv4 address, followed by a forward slash, then the prefix length. This matches any destination IP address within the specified subnet.
	<ip-addr>	An IPv4 address in a.b.c.d format.
exact-match	Specify an exact IP prefix to match on.	
any	Matches any source IP address.	

Mode IPv4 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list standard (named) command with the required access control list name, but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples Use the following commands to add a new filter entry to access-list `my-list` that will reject IP address `10.1.1.1`:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# deny 10.1.1.1/32
```

Use the following commands to insert a new filter entry into access-list `my-list` at sequence position number `15` that will accept IP network `10.1.2.0`:

```
awplus# configure terminal
awplus(config)# access-list standard my-list
awplus(config-ip-std-acl)# 15 permit 10.1.2.0/24
```

Related Commands access-list standard (named)

show running-config

show ip access-list

(access-list standard numbered filter)

Overview This ACL filter adds a source IP address filter entry to a current standard numbered access-list. If a sequence number is specified, the new filter entry is inserted at the specified location. Otherwise, the new filter entry is added at the end of the access-list.

The **no** variant of this command removes a source IP address filter entry from the current standard numbered access-list. You can specify the source IP address filter entry for removal by entering either its sequence number (e.g. `no 10`), or by entering its source IP address filter profile without specifying its sequence number.

Note that the sequence number can be found by running the show access-list (IPv4 Software ACLs) command.

Syntax

```
[<sequence-number>] {deny|permit} {<source>|host
<host-address>|any}
no {deny|permit} {<source>|host <host-address>|any}
no <sequence-number>
```

Parameter	Description	
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.	
deny	Access-list rejects packets of the type specified.	
permit	Access-list allows packets of the type specified	
<source>	The source address of the packets. You can specify either a subnet or all sources. The following are the valid formats for specifying the source:	
	<ip-addr> <reverse-mask>	Enter a reverse mask for the source address in dotted decimal format. For example, entering `192.168.1.1 0.0.0.255` is the same as entering `192.168.1.1/24`.
	<ip-addr>	An IPv4 address in a.b.c.d format.
host	A single source host.	
<host-address>	Single source host address.	
any	Matches any source IP address.	

Mode IPv4 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage An ACL can be configured with multiple ACL filters using sequence numbers. If the sequence number is omitted, the next available multiple of 10 will be used as the sequence number for the new filter. A new ACL filter can be inserted into the middle of an existing list by specifying the appropriate sequence number.

NOTE: *The access control list being configured is selected by running the access-list (standard numbered) command with the required access control list number but with no further parameters selected.*

*Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example To add a new entry accepting the IP network `10.1.1.0/24` at the sequence number `15` position, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 99
awplus(config-ip-std-acl)# 15 permit 10.1.2.0 0.0.0.255
```

Related Commands access-list (standard numbered)

show running-config

show ip access-list

clear ip prefix-list

Overview Use this command to reset the hit count to zero in the prefix-list entries.

Syntax

```
clear ip prefix-list [<list-name>] [<ip-address>/<mask>]
```

Parameter	Description
<list-name>	The name of the prefix-list.
<ip-address>/<mask>	The IP prefix and length.

Mode Privileged Exec

Example To clear a prefix-list named List1:

```
awplus# clear ip prefix-list List1
```

dos

Overview Use this command to configure Denial-of-Service (DoS) features for a port. Six different DoS attacks can be detected: IP Options, Land, Ping-of-Death, Smurf, Synflood and Teardrop.

When the attack is detected, three different actions are available:

- Shutdown the port for one minute
- Cause an SNMP trap.
- Send traffic to the mirror port

Syntax

```
dos {ipoptions|land|ping-of-death|smurf broadcast
<ip-address>|synflood|teardrop} action {shutdown|trap|mirror}
```

Parameter	Description
`dos`	Denial-Of-Service.
`ipoptions`	IP Options attack.
`land`	Land attack.
`ping-of-death`	Large ping attack.
`smurf`	Ping to broadcast address.
`broadcast`	Broadcast.
<ip-address>	Local IP Broadcast Address.
`synflood`	SYN flood attack.
`teardrop`	IP fragmentation attack.
`action`	Action.
`shutdown`	Shutdown port.
`trap`	Trap to SNMP.
`mirror`	Send packets to mirror port.

Mode Interface Configuration for a switch port interface.

Default DoS attack detection is not configured by default on any switch port interface.

Usage See the below table for more information about the DoS attacks recognized by this command:

Type of DoS attack	Description
ipoptions	This type of attack occurs when an attacker sends packets containing bad IP options to a victim node. There are many different types of IP options attacks and this software does not try to distinguish between them. Rather, if this defense is activated, the number of ingress IP packets containing IP options is counted. If the number exceeds 20 packets per second, the switch considers this a possible IP options attack. This defense does not require the CPU to monitor packets, so does not put extra load on the switch's CPU.
land	This type of attack occurs when the Source IP and Destination IP address are the same. This can cause a target host to be confused. Since packets with the same source and destination addresses should never occur, these packets are dropped when this attack is enabled. This defense does not require the CPU to monitor packets, so does not put extra load on the switch's CPU.
ping-of-death	This type of attack results from a fragmented packet which, when reassembled, would exceed the maximum size of a valid IP datagram. To detect this attack, the final fragment of ICMP packets has to be sent to the CPU for inspection. This defense can therefore load the CPU. Note that the extra CPU load will not affect normal traffic switching between ports, but other protocols such as IGMP and STP may be affected. This defense is not recommended where a large number of fragmented packets are expected.
smurf	This type of attack is an ICMP ping packet to a broadcast address. Although routers should not forward packets to local broadcast addresses anymore (see RFC2644), the Smurf attack can still be explicitly discarded with this command. In order for the Smurf attack to work, the broadcast IP address is required. Any ICMP Ping packet with this destination address is considered an attack. This defense does not require the CPU to monitor packets, so does not put extra load on the switch's CPU.
synflood	In this type of attack, an attacker, seeking to overwhelm a victim with TCP connection requests, sends a large number of TCP SYN packets with bogus source addresses to the victim. The victim responds with SYN ACK packets, but since the original source addresses are bogus, the victim node does not receive any replies. If the attacker sends enough requests in a short enough period, the victim may freeze operations once the requests exceed the capacity of its connections queue. To defend against this form of attack, a switch port monitors the number of ingress TCP-SYN packets it receives. An attack is recorded if a port receives more 60 TCP-SYN packets per second.
teardrop	In this DoS attack, an attacker sends a packet in several fragments with a bogus offset value, used to reconstruct the packet, in one of the fragments to a victim. This results in the victim being unable to reassemble the packet, possibly causing it to freeze operations.

Examples

To configure **smurf** DoS detection on `port1.0.1`, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos smurf broadcast 192.168.1.0 action shutdown
```

To configure **land** DoS detection on `port1.0.1`, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos land action shutdown
```

To configure **ipoptions** DoS detection on `port1.0.1`, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos ipoptions action shutdown
```

To configure **ping-of-death** DoS detection on `port1.0.1`, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos ping-of-death action shutdown
```

To configure **synflood** DoS detection on `port1.0.1`, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos synflood action shutdown
```

To configure **teardrop** DoS detection on `port1.0.1`, and shutdown the interface if an attack is detected, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# dos teardrop action shutdown
```

Related Commands

show dos interface

maximum-access-list

Overview Sets the maximum number of filters that can be added to any access-list. These are access-lists within the ranges <1-199>, <1300-1999> and <2000-2699> and named standard and extended access-lists.

The **no** variant of this command removes the limit on the number of filters that can be added to a software access-list

Syntax

```
maximum-access-list <1-4294967294>
no maximum-access-list
```

Parameter	Description
<1-4294967294>	Filter range.

Mode Global Configuration

Example To set the maximum number of software filters to `200`:

```
awplus# configure terminal
awplus(config)# maximum-access-list 200
```

show access-list (IPv4 Software ACLs)

Overview Use this command to display the specified access-list, or all access-lists if none have been specified. Note that only defined access-lists are displayed. An error message is displayed for an undefined access-list

Syntax

```
show access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<3000-3699>|
<4000-4499>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (standard - expanded range).
<2000-2699>	IP extended access-list (extended - expanded range).
<3000-3699>	Hardware IP access-list.
<4000-4499>	Hardware MAC access-list.
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Examples To show all access-lists configured on the switch:

```
awplus# show access-list
```

```
Standard IP access list 1
    deny 172.16.2.0, wildcard bits 0.0.0.255
Standard IP access list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
Hardware IP access list 3001
    permit ip 192.168.20.0 255.255.255.0 any
Hardware IP access list 3020
    permit tcp any 192.0.2.0/24
awplus#show access-list 20
```

To show the access-list with an ID of 20:

```
awplus# show access-list 20
```

```
Standard IP access-list 20
    deny 192.168.10.0, wildcard bits 0.0.0.255
    deny 192.168.12.0, wildcard bits 0.0.0.255
```

Note the following error message is displayed if you attempt to show an undefined access-list:

```
awplus# show access-list 2
```

```
% Can't find access-list 2
```

Related Commands

access-list standard (named)

access-list (standard numbered)

access-list (extended numbered)

show dos interface

Overview Use this command to display the Denial-of-Service (DoS) features configured on a switch port interface from the dos command. See the dos command for descriptions of DoS attack types.

Syntax `show dos interface {<port-list>}`

Parameter	Description
<port-list>	Specify the switch port or port list to display DoS configuration options set with the dos command.

Mode Privileged Exec

Output Figure 25-1: Example output from the **show dos interface** command prior to a DoS attack

```
awplus#configure terminal
Enter configuration commands, one per line. End with CTNTL/Z.
awplus(config)#interface port1.0.1
awplus(config-if)#dos synflood action shutdown
awplus(config-if)#exit
awplus(config)#exit
awplus#show dos interface port1.0.1

DoS settings  for interface port1.0.1
----------------------------------------
Port status          : Enabled
ipoptions            : Disabled
land                 : Disabled
ping-of-death        : Disabled
smurf                : Disabled
synflood             : Enabled
   Action            : Shutdown port
   Attacks detected  : 0
teardrop             : Disabled
awplus#
```

Figure 25-2: Example output from the **show dos interface** command after a **synflood** DoS attack

```
awplus#show dos interface port1.0.1

DoS settings for interface port1.0.1
----------------------------------------
Port status          : Enabled
ipoptions            : Disabled
land                 : Disabled
ping-of-death        : Disabled
smurf                : Disabled
synflood             : Enabled
   Action            : Shutdown port
   Attacks detected  : 1
teardrop             : Disabled
awplus#
```

Table 26: Parameters in the **show dos interface** command output:

Type of DoS attack	Description
`Port status`	Displays `Enabled` when the port is configured as being administratively up after issuing the **no shutdown** command. Displays `Disabled` when the port is configured as being administratively down with the **shutdown** command.
`ipoptions`	Displays `Enabled` when the **ipoptions** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **ipoptions** DoS attacks that have occurred on the interface. Displays `Disabled` when the **ipoptions** parameter is not configured with the dos command.
`land`	Displays `Enabled` when the **land** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **land** DoS attacks that have occurred on the interface. Displays `Disabled` when the **land** parameter is not configured with the dos command.
`ping-of-death`	Displays `Enabled` when the **ping-of-death** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **ping-of-death** DoS attacks that have occurred on the interface. Displays `Disabled` when the **ping-of-death** parameter is not configured with the dos command.

Table 26: Parameters in the **show dos interface** command output: (cont.)

Type of DoS attack	Description
`smurf`	Displays `Enabled` when the **smurf** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **smurf** DoS attacks that have occurred on the interface. Displays `Disabled` when the **smurf** parameter is not configured with the dos command.
`synflood`	Displays `Enabled` when the **synflood** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **synflood** DoS attacks that have occurred on the interface. Displays `Disabled` when the **synflood** parameter is not configured with the dos command.
`teardrop`	Displays `Enabled` when the **teardrop** parameter is configured with the dos command, plus the action (`Shutdown port`, `Mirror port`, or `Trap port`) and the number of instances of any **teardrop** DoS attacks that have occurred on the interface. Displays `Disabled` when the **teardrop** parameter is not configured with the dos command.

Related Commands dos

show ip access-list

Overview Use this command to display IP access-lists.

Syntax
```
show ip access-list
[<1-99>|<100-199>|<1300-1999>|<2000-2699>|<access-list-name>]
```

Parameter	Description
<1-99>	IP standard access-list.
<100-199>	IP extended access-list.
<1300-1999>	IP standard access-list (expanded range).
<2000-2699>	IP extended access-list (expanded range).
<access-list-name>	IP named access-list.

Mode User Exec and Privileged Exec

Example
```
awplus# show ip access-list
```

Output Figure 25-3: Example output from the **show ip access-list** command

```
Standard IP access-list 1
    permit 172.168.6.0, wildcard bits 0.0.0.255
    permit 192.168.6.0, wildcard bits 0.0.0.255
```

vty access-class (numbered)

Overview For IPv4, use this command to set a standard numbered software access list to be the management ACL. This is then applied to all available VTY lines for controlling remote access by Telnet and SSH. This command allows or denies packets containing the IP addresses included in the ACL to create a connection to your device.

ACLs that are attached using this command have an implicit deny-all filter as the final entry in the ACL. So a typical configuration would be to permit a specific address, or range of addresses, and rely on the deny-all filter to block all other access.

Use the **no** variant of this command to remove the access list.

Syntax

```
vty access-class {<1-99>|<1300-1999>}
no vty access-class [<1-99>|<1300-1999>]
```

Parameter	Description
<1-99>	IPv4 standard access-list number
<1300-1999>	IPv4 standard access-list number (expanded range)

Mode Global Configuration

Examples To set access-list 4 to be the management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# vty access-class 4
```

To remove access-list 4 from the management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# no vty access-class 4
```

Output Figure 25-4: Example output from the **show running-config** command

```
awplus#show running-config|grep access-class

vty access-class 4
```

Related Commands

show running-config

vty ipv6 access-class (named)

26 IPv6 Hardware Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference for the IPv6 Hardware Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 hardware ACLs, which are applied directly to interfaces using the ipv6 traffic-filter command.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview and Configuration Guide.
- Link Aggregation Commands

Note that text in parenthesis in command names indicates usage not keyword entry. For example, **ipv6-access-list (named)** indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where <*name*> is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI, such as **(ipv6 access-list standard IPv6 filter)** represents command entry in the format shown in the syntax [<*sequence-number*>] {deny|permit} {<*IPv6-source-address/prefix-length*>|any}.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 26-1: IPv6 Hardware Access List Commands and Prompts

Command Name	Command Mode	Prompt
show ipv6 access-list (IPv6 Hardware ACLs)	Privileged Exec	awplus#
ipv6 access-list (named)	Global Configuration	awplus(config)#
(ipv6 access-list named ICMP filter)	Global Configuration	awplus(config)#
ipv6 traffic-filter	Interface Configuration	awplus(config-if)#
commit (IPv6)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(ipv6 access-list named ICMP filter)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(ipv6 access-list named protocol filter)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#
(ipv6 access-list named TCP UDP filter)	IPv6 Hardware ACL Configuration	awplus(config-ipv6-hw-acl)#

Command List

commit (IPv6)

Overview Use this command to commit the IPv6 ACL filter configuration entered at the console to the hardware immediately without exiting the IPv6 Hardware ACL Configuration mode.

This command forces the associated hardware and software IPv6 ACLs to synchronize.

Syntax

```
commit
```

Mode IPv6 Hardware ACL Configuration

Usage Normally, when an IPv6 hardware ACL is edited, the new configuration state of the IPv6 ACL is not written to hardware until you exit IPv6 Hardware ACL Configuration mode. By entering this command you can ensure that the current state of a hardware access-list that is being edited is written to hardware immediately.

Scripts typically do not include the exit command to exit configuration modes, potentially leading to IPv6 ACL filters in hardware not being correctly updated. Using this **commit** command in a configuration script after specifying an IPv6 hardware ACL filter ensures that it is updated in the hardware.

Example To update the hardware with the IPv6 ACL filter configuration, use the command:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)# commit
```

Related Commands ipv6 access-list (named)

ipv6 access-list (named)

Overview Use this command to either create a new IPv6 hardware access-list, or to select an existing IPv6 hardware access-list in order to apply a filter entry to it.

Use the **no** variant of this command to delete an existing IPv6 hardware access-list.

NOTE: *Before you can delete an access-list, you must first remove it from any interface it is assigned to.*

Syntax

```
ipv6 access-list <ipv6-access-list-name>
no ipv6 access-list <ipv6-access-list-name>
```

Parameter	Description
<ipv6-access-list-name>	Specify an IPv6 access-list name.

Mode Global Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicitly match a filter is permitted.

Usage Use IPv6 hardware named access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 hardware named access-list when a match is encountered.

For backwards compatibility you can either create IPv6 hardware named access-lists from within this command, or you can enter `ipv6 access-list` followed by only the IPv6 hardware named access-list name. This latter (and preferred) method moves you to the `(config-ipv6-hw-acl)` prompt for the selected IPv6 hardware named access-list number, and from here you can configure the filters for this selected IPv6 hardware named access-list.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To create an IPv6 access-list named `my-ipv6-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-ipv6-acl
awplus(config-ipv6-hw-acl)#
```

To delete the IPv6 access-list named `my-ipv6-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 access-list my-ipv6-acl
```

Validation Commands show ipv6 access-list (IPv6 Hardware ACLs)

Related Commands

(ipv6 access-list named ICMP filter)

(ipv6 access-list named protocol filter)

(ipv6 access-list named TCP UDP filter)

ipv6 traffic-filter

show ipv6 access-list (IPv6 Hardware ACLs)

(ipv6 access-list named ICMP filter)

Overview

Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with ICMP (Internet Control Message Protocol) packets, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the **send-to-cpu** parameter could result in EPSR healthcheck messages and other control packets being dropped.

As an optional parameter **vlan** can be matched for tagged (802.1q) packet.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with ICMP (Internet Control Message Protocol) packets, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Syntax [ip|icmp]

```
[<sequence-number>
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|
copy-to-mirror} {ipv6|icmp}
{<ipv6-source-address/prefix-length>|
<ipv6-source-address> <ipv6-source-wildcard>|
host <ipv6-source-host>|any}
{<ipv6-destination-address/prefix-length>|
<ipv6-destintation-addr> <ipv6-destination-wildcard>|
host <ipv6-destination-host-address>|any}
[<icmp-type>] [vlan <1-4094>]
```

```
no [<sequence-number>]
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|
copy-to-mirror} {ip|icmp}
{<ipv6-source-address/prefix-length>|
<ipv6-source-address> <ipv6-source-wildcard>|
host <ipv6-source-host>|any}
{<ipv6-destination-address/prefix-length>|
<ipv6-destination-address> <ipv6-destination-wildcard>|
host <ipv6-destination-host-address>|any}
[<icmp-type>] [vlan <1-4094>]
```

```
no [<sequence-number>]
```

Parameter	Description
<*sequence-number*>	<1-65535>The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to permit.

Parameter	Description
`send-to-cpu`	Specifies the packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.
`send-to-mirror`	Specifies the packets to send to mirror port.
`copy-to-cpu`	Specifies the packets to copy to the CPU.
`copy-to-mirror`	Specifies the packets to copy to the mirror port.
`ipv6`	IPv6 packet, defined by the following parameters.
`icmp`	ICMP packet, defined by the following parameters.
<ipv6-source-address/ prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<ipv6-source-address>	Specifies the IPv6 source address. The IPv6 address uses the format X:X::X:X.
<ipv6-source-wildcard>	Specifies source wildcard bits in IPv6 format X:X::X:X. Note that binary 1 represents a don't care condition, and binary 0 represents a match.
`host` *<ipv6-source-host>*	Specifies a single source host address. The IPv6 address uses the format X:X::X:X.
`any`	Specifies any Source host.
<ipv6-destination-address/prefix-length>	Specifies a destination address and prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<ipv6-destination-addrress>	Specifies a destination address. The IPv6 address uses the format X:X::X:X.
<ipv6-destination-wildcard>	Specify destination wildcard bits in IPv6 format X:X::X:X.
`host` *<ipv6-destination-host-address>*	Specify a single destination host address. The IPv6 address uses the format X:X::X:X.
`any`	Specifies any destination host.
<icmp-type>	Optional. Specify to filter by ICMP message type number. Valid values are from 0 to 255.

Parameter	Description
`vlan`	This parameter can be used in either single or double-tagged VLAN networks. It is the conventional VLAN tag (VID). In a double-tagged network it is sometimes referred to as the STAG.
<1-4094>	The VLAN VID.

Mode IPv6 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

Examples To specify a hardware IPv6 access-list named`my-acl1` and add an ACL filter entry that blocks all ICMP6 echo requests, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
```

To specify a hardware IPv6 access-list named `my-acl2`and add an ACL filter entry that blocks all ICMP6 echo requests on the default VLAN (`vlan1`), enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl2
awplus(config-ipv6-hw-acl)# deny icmp any any icmp-type 128
vlan 1
```

To remove an ACL filter entry that blocks all ICMP6 echo requests from he hardware IPv6 access-list named `my-acl1`, enter the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl1
awplus(config-ipv6-hw-acl)# no deny icmp any any icmp-type 128
```

Related Commands

ipv6 access-list (named)

(ipv6 access-list named protocol filter)

(ipv6 access-list named TCP UDP filter)

ipv6 traffic-filter

show ipv6 access-list (IPv6 Hardware ACLs)

(ipv6 access-list named protocol filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the **send-to-cpu** parameter could result in EPSR healthcheck messages and other control packets being dropped.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with an IP protocol type specified, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax

```
[<sequence-number>
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|
copy-to-mirror} {ipv6|proto <ip-protocol>}
{<ipv6-source-prefix/prefix-length>|
<ipv6-source-address> <ipv6-source-wildcard>|
host <ipv6-source-host>|any}
{<ipv6-destination-prefix/prefix-length>|
<ipv6-destination-address> <ipv6-destination-wildcard>|
host <ipv6-destination-host>|any}

no [<sequence-number>]
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|
copy-to-mirror} {ipv6|proto <ip-protocol>}
{<ipv6-source-prefix/prefix-length>|
<ipv6-source-address> <ipv6-source-wildcard>|
host <ipv6-source-host>|any}
{<ipv6-destination-prefix/prefix-length>|
<ipv6-destination-address> <ipv6-destination-wildcard>|
host <ipv6-destination-host>|any}

no [<sequence-number>]
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies packets to reject.
permit	Specifies packets to permit.
send-to-cpu	Specifies packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.
send-to-mirror	Specifies packets to send to mirror port.
copy-to-cpu	Specifies packets to copy to the CPU.
copy-to-mirror	Specifies packets to copy to the mirror port.

Parameter	Description
`ipv6`	Specifies IPv6 packet.
`proto <ip-protocol>`	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.
`<ipv6-source-prefix/prefix-length>`	Specify source address and mask. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`<ipv6-source-address>`	Specifies the source address. The IPv6 address uses the format X:X::X:X.
`<ipv6-source-wildcard>`	Specifies the source wildcard bits, in IPv6 format X:X::X:X.
`host <ipv6-source-host>`	Specifies a single source host. The IPv6 address uses the format X:X::X:X.
`any`	Specifies any source host. An abbreviation for the IPv6 prefix ::/0
`<ipv6-dest-prefix/prefix-length>`	Specifies a destination address and mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
`<ipv6-destination-address>`	Specify destination address. The IPv6 address uses the format X:X::X:X.
`<ipv6-destination-wildcard>`	Specify destination wildcard bits in IPv6 format X:X::X:X
`host <ipv6-destination-host>`	Specify a single destination host address. The IPv6 address uses the format X:X::X:X.
`any`	Specifies any destination host. An abbreviation for the IPv6 prefix ::/0
`vlan`	This parameter can be used in either single or double-tagged VLAN networks. It is the conventional VLAN tag (VID). In a double-tagged network it is sometimes referred to as the STAG.
`<1-4094>`	The VLAN VID.

Table 26-2: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]

Table 26-2: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv6 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

Usage This command adds a hardware classification filter (for use with features such as QoS), to a current standard IPv6 access-list. The filter will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter,

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To add an ACL filter entry to block IP traffic from network `2001:0db8::0/64` to the hardware IPv6 access-list named `my-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny ipv6 2001:0db8::0/64
```

To remove an ACL filter entry that blocks all IPv6 traffic from network `2001:0db8::0/ 64` from the hardware IPv6 access-list named `my-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny ipv6 2001:0db8::0/64
```

Related Commands

ipv6 access-list (named)

(ipv6 access-list named ICMP filter)

(ipv6 access-list named TCP UDP filter)

ipv6 traffic-filter

show ipv6 access-list (IPv6 Hardware ACLs)

(ipv6 access-list named TCP UDP filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination ports specified, to the current named IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

Note that specifying the **send-to-cpu** parameter could result in EPSR healthcheck messages and other control packets being dropped.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with TCP or UDP source and destination ports specified, from the current named IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax

```
[<sequence-number>]
{deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|
copy-to-mirror} {tcp|udp} {<ipv6-source-prefix/prefix-length>|
<ipv6-source-address> <ipv6-source-wildcard>|
host <ipv6-source-host>|any}
{eq <sourceport>|lt <sourceport>|gt <sourceport>|
ne <sourceport>|range <start-range> <end-range>]}
{<ipv6-destination-prefix/prefix-length>|
<ipv6-destination-address> <ipv6-destination-wildcard>|
host <ipv6-destination-host>|any}
{[eq <destport>|lt <destport>|gt <destport>|
ne <destport>|range <start-range> <end-range>]}
```

```
no {deny|permit|send-to-cpu|send-to-mirror|copy-to-cpu|
copy-to-mirror} {tcp|udp} {<ipv6-source-prefix/prefix-length>|
<ipv6-source-address> <ipv6-source-wildcard>|
host <ipv6-source-host>|any}
{eq <sourceport>|lt <sourceport>|gt <sourceport>|
ne <sourceport>|range <start-range> <end-range>]}
{<ipv6-destination-prefix/prefix-length>|
<ipv6-destination-address> <ipv6-destination-wildcard>|
host <ipv6-destination-host>|any}
{eq <destport>|lt <destport>|gt <destport>|
ne <destport>}|range <start-range> <end-range>}
```

```
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535>The sequence number for the filter entry of the selected access control list.
deny	Specify packets to reject.
permit	Specifies the packets to permit.

Parameter	Description
`send-to-cpu`	Specifies the packets to send to the CPU. Specifying this parameter could result in EPSR healthcheck messages and other control packets being dropped.
`send-to-mirror`	Specifies the packets to send to mirror port.
`copy-to-cpu`	Specifies the packets to copy to the CPU.
`copy-to-mirror`	Specifies the packets to copy to the mirror port.
`tcp`	Specifies a TCP packet.
`udp`	Specifies a UDP packet.
<ipv6-source-prefix/ prefix-length>	Specifies the source address with mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<ipv6-source-address>	Specifies the source address. The IPv6 address uses the format X:X::X:X.
<ipv6-source-wildcard>	Specifies the source wildcard bits in IPv6 format X:X::X:X.
`host` *<ipv6-source-host>*	Specifies the a single source host. The IPv6 address uses the format X:X::X:X.
`any`	Specifies any Source host. An abbreviation for the IPv6 prefix ::/0.
`eq`	Equal to.
`lt`	Less than.
`gt`	Greater than.
`ne`	Not equal to.
<sourceport>	The source port number, specified as an integer between 0 and 65535.
<destport>	The destination port number, specified as an integer between 0 and 65535.
`range`	Range of port numbers. Match only packets within range.
<start-range>	The port number at the start of the range *<0-65535>*.
<end-range>	The port number at the end of the range *<0-65535>*.
<ipv6-dest-prefix/ prefix-length>	Specify destination address with mask. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<ipv6-destination-address>	Specify destination address. The IPv6 address uses the format X:X::X:X.

Parameter	Description
<ipv6-destination-wildcard>	Specify destination wildcard bits in IPv6 format X:X::X:X.
host *<ipv6-destination-host>*	Specify a single destination host address. The IPv6 address uses the format X:X::X:X.
any	Specifies any destination host. An abbreviation for the IPv6 prefix **::/0**.

Mode IPv6 Hardware ACL Configuration

Default Any traffic on an interface controlled by a hardware ACL that does not explicate match a filter is permitted.

Usage The filter entry will match on any TCP or UDP packet that has the specified source and destination IPv6 addresses and TCP or UDP type. The parameter `any` may be specified if an address does not matter.

NOTE: *Hardware ACLs will **permit** access unless **explicitly denied** by an ACL action.*

Examples To add an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 to the hardware IPv6 access-list named `my-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny tcp 2001:0db8::0/64 any eq 22
```

To add an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 on the default VLAN (`vlan1`) to the hardware IPv6 access-list named `my-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# deny tcp 2001:0db8::0/64 any eq 22
vlan 1
```

To remove an ACL filter entry that blocks all SSH traffic from network 2001:0db8::0/64 from the hardware IPv6 access-list named `my-acl`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list my-acl
awplus(config-ipv6-hw-acl)# no deny tcp 2001:0db8::0/64 any eq
22
```

Related Commands

ipv6 access-list (named)

(ipv6 access-list named ICMP filter)

(ipv6 access-list named protocol filter)

ipv6 traffic-filter

show ipv6 access-list (IPv6 Hardware ACLs)

ipv6 traffic-filter

Overview This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

Use the **no** variant of this command to remove an IPv6 hardware-based access-list from an interface.

Syntax

```
ipv6 traffic-filter <ipv6-access-list-name>
no ipv6 traffic-filter <ipv6-access-list-name>
```

Parameter	Description
<ipv6-access-list-name>	Hardware IPv6 access-list name.

Mode Interface Configuration (to apply an IPv6 hardware ACL to a specific switch port).

Usage This command adds an IPv6 hardware-based access-list to an interface. The number of access-lists that can be added is determined by the amount of available space in the hardware-based packet classification tables.

To apply the access-list to all ports on the switch, execute the command in the Global Configuration mode. To apply the access-list to a Layer 2 interface or Layer 2 interface range, apply the command in the Interface Configuration mode. See the examples for each mode below.

Examples To add access-list `acl1` as a traffic-filter to interface `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# ipv6 traffic-filter acl1
```

To remove access-list `acl1` as a traffic-filter from interface `port1.0.1`, enter the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no ipv6 traffic-filter acl1
```

Related Commands

ipv6 access-list (named)

(ipv6 access-list named ICMP filter)

(ipv6 access-list named protocol filter)

(ipv6 access-list named TCP UDP filter)

ipv6 traffic-filter

show ipv6 access-list (IPv6 Hardware ACLs)

show ipv6 access-list (IPv6 Hardware ACLs)

Overview Use this command to display all configured hardware IPv6 access-lists or the IPv6 access-list specified by name. Omitting the optional access-list name parameter will display all IPv6 ACLs.

Use the **show ipv6 access-list standard** command to display the IPv6 access-list specified by name as defined from the ipv6 access-list (named) command.

Syntax

```
show ipv6 access-list [<access-list-name>]
show ipv6 access-list standard [<access-list-name>]
```

Parameter	Description
`standard`	Named standard access-list.
`<access-list-name>`	Hardware IPv6 access-list name.

Mode User Exec and Privileged Exec

Examples To show the standard named ipv6 access-list acl_name use the following command:

```
awplus# show ipv6 access-list standard acl_name
```

Output Figure 26-1: Example output from the **show ipv6 access-list standard** command

```
Named Standard IPv6 access-list acl_name
  deny any
```

To show all configured ipv6 access-lists use the command:

```
awplus# show ipv6 access-list
```

Output Figure 26-2: Example output from the **show ipv6 access-list** command

```
IPv6 access-list deny_icmp
  deny icmp any any vlan 1

IPv6 access-list deny_ssh
  deny tcp abcd::0/64 any eq 22
```

Related Commands

ipv6 access-list (named)

(ipv6 access-list named ICMP filter)

(ipv6 access-list named protocol filter)

(ipv6 access-list named TCP UDP filter)

ipv6 traffic-filter

27 IPv6 Software Access Control List (ACL) Commands

Introduction

Overview This chapter provides an alphabetical reference for the IPv6 Software Access Control List (ACL) commands, and contains detailed command information and command examples about IPv6 software ACLs as applied to Routing and Multicasting, which are not applied to interfaces.

For information about ACLs, see the ACL Feature Overview and Configuration Guide.

To apply ACLs to an LACP channel group, apply it to all the individual switch ports in the channel group. To apply ACLs to a static channel group, apply it to the static channel group itself. For more information on link aggregation see the following references:

- the Link Aggregation Feature Overview and Configuration Guide.
- Link Aggregation Commands

Note that text in parenthesis in command names indicates usage not keyword entry. For example, **ipv6-access-list (named)** indicates named IPv6 ACLs entered as `ipv6-access-list <name>` where <*name*> is a placeholder not a keyword.

Note also that parenthesis surrounding ACL filters indicates the type of ACL filter not the keyword entry in the CLI. For example, **(ipv6 access-list standard IPv6 filter)** represents command entry in the format:

[<*sequence-number*>] {deny|permit} {<*IPv6-source-address/prefix-length*>|any}.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Sub-modes Many of the ACL commands operate from sub-modes that are specific to particular ACL types. The following table shows the CLI prompts at which ACL commands are entered.

Table 27-1: IPv6 Software Access List Commands and Prompts

Command Name	Command Mode	Prompt
show ipv6 access-list (IPv6 Software ACLs)	Privileged Exec	`awplus#`
ipv6 access-list extended (named)	Global Configuration	`awplus(config)#`
ipv6 access-list standard (named)	Global Configuration	`awplus(config)#`
(ipv6 access-list extended IP protocol filter)	IPv6 Extended ACL Configuration	`awplus(config-ipv6-ext-acl)#`
(ipv6 access-list extended TCP UDP filter)	IPv6 Extended ACL Configuration	`awplus(config-ipv6-ext-acl)#`
(ipv6 access-list standard filter)	IPv6 Standard ACL Configuration	`awplus(config-ipv6-std-acl)#`

Command List

ipv6 access-list extended (named)

Overview

Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny IP, ICMP, TCP, UDP packets or ICMP packets with a specific value based on the source or destination.

The **no** variant of this command removes a specified IPv6 extended access-list.

Syntax [list-name]

```
ipv6 access-list extended <list-name>
no ipv6 access-list extended <list-name>
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.

Syntax [any|icmp|ip]

```
ipv6 access-list extended <list-name> {deny|permit}
{any|icmp|ip} {<ipv6-source-address/prefix-length>|any}
{<ipv6-destination-address/prefix-length>|any} [<icmp-type
<icmp-type>][log]
no ipv6 access-list extended <list-name> {deny|permit}
{any|icmp|ip} {<ipv6-source-address/prefix-length>|any}
{<ipv6-destination-address/prefix-length>|any} [<icmp-type
<icmp-type>][log]
```

Syntax [tcp|udp]

```
ipv6 access-list extended <list-name> {deny|permit} {tcp|udp}
{<ipv6-source-address/prefix-length>|any} {eq <sourceport>|lt
<sourceport>|gt <sourceport>|ne
<sourceport>}{<ipv6-destination-address/prefix-length>|any}
{eq <destport>|lt <destport>|gt <destport>|ne <destport>} [log]
no ipv6 access-list extended <list-name> {deny|permit}
{tcp|udp} {<ipv6-source-address/prefix-length>|any} {eq
<sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>}{<ipv6-destination-addr/prefix-length>|any} {eq
<destport>|lt <destport>|gt <destport>|ne <destport>} [log]
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access-list.
deny	The IPv6 software extended access-list rejects packets that match the type, source, and destination filtering specified with this command.
permit	The IPv6 software extended access-list permits packets that match the type, source, and destination filtering specified with this command.

Parameter	Description
any	For ICMP|IP The IPv6 software extended access-list matches any type of packet.
ip	For ICMP|IP The IPv6 software extended access-list matches only IP packets.
icmp	For ICMP|IP The IPv6 software extended access-list matches only ICMP packets.
tcp	For TCP/UDP The IPv6 software extended access-list matches only TCP packets.
udp	For TCP/UDP The IPv6 software extended access-list matches only UDP packets.
<ipv6-source-address/prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
<ipv6-destination-address/prefix-length>	Specifies a destination address and prefix length. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Matches any IPv6 address.
<sourceport>	For TCP/UDP The source port number, specified as an integer between 0 and 65535.
<destport>	For TCP/UDP The destination port number, specified as an integer between 0 and 65535.
icmp-type	For ICMP|IP Matches only a specified type of ICMP messages. This is valid only when the filtering is set to match ICMP packets.
eq	For TCP/UDP Matches port numbers equal to the port number specified immediately after this parameter.
lt	For TCP/UDP Matches port numbers less than the port number specified immediately after this parameter.
gt	For TCP/UDP Matches port numbers greater than the port number specified immediately after this parameter.
ne	For TCP/UDP Matches port numbers not equal to the port number specified immediately after this parameter.

Parameter	Description	
<icmp-type>	For ICMP|IP The ICMP type, as defined in RFC792 and RFC950. Specify one of the following integers to create a filter for the ICMP message type:	
	0	Echo replies.
	3	Destination unreachable messages.
	4	Source quench messages.
	5	Redirect (change route) messages.
	8	Echo requests.
	11	Time exceeded messages.
	12	Parameter problem messages.
	13	Timestamp requests.
	14	Timestamp replies.
	15	Information requests.
	16	Information replies.
	17	Address mask requests.
	18	Address mask replies.
`log`	Logs the results.	

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use IPv6 extended access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 extended access-list when a match is encountered.

For backwards compatibility you can either create IPv6 extended access-lists from within this command, or you can enter `ipv6 access-list extended` followed by only the IPv6 extended access-list name. This latter (and preferred) method moves you to the `(config-ipv6-ext-acl)` prompt for the selected IPv6 extended access-list number, and from here you can configure the filters for this selected access-list.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example 1 [creating a list]

To add a new filter to the access-list named `my-list` that will reject incoming ICMP packets from 2001:0db8::0/64 to 2001:0db8::f/64, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# icmp 2001:0db8::0/64
2001:0db8::f/64
```

Example 2 [adding to a list]

To insert a new filter at sequence number `5` of the access-list named `my-list`that will accept ICMP type 8 packets from the 2001:0db8::0/64 network to the 2001:0db8::f/64 network, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 icmp 2001:0db8::0/64
2001:0db8::f/64
```

Example 3 [list with filter]

To create the access-list named TK to deny TCP protocols, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended TK deny tcp any eq 14
any lt 12 log
```

Related Commands

ipv6 access-list extended proto

(ipv6 access-list extended IP protocol filter)

(ipv6 access-list extended TCP UDP filter)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

ipv6 access-list extended proto

Overview Use this command when configuring an IPv6 extended access-list for filtering frames that permit or deny packets with a specific value based on the IP protocol number specified.

The **no** variant of this command removes a specified IPv6 extended access-list with an IP protocol number.

Syntax

```
ipv6 access-list extended <list-name> {deny|permit} proto
<ip-protocol>} {<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]
```

```
no ipv6 access-list extended <list-name> {deny|permit} proto
<ip-protocol>{<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]
```

Parameter	Description
<list-name>	A user-defined name for the IPv6 software extended access- list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
proto	The IP Protocol type specified by its protocol number in the range 1 to 255.
<ip-protocol>	The IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any destination address or remote address.
log	Log the results.

Table 27-2: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]

Table 27-2: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt

Table 27-2: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use IPv6 extended access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 extended access-list when a match is encountered.

The filter entry will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To create the IPv6 access-list named `ACL-1` to deny IP protocol `9` packets from `2001:0db8:1::1/128` to `2001:0db8:f::1/128`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended ACL-1 deny proto 9
2001:0db8:1::1/128 2001:0db8:f::1/128
```

To remove the IPv6 access-list named `ACL-1` to deny IP protocol `9` packets from `2001:0db8:1::1/128` to `2001:0db8:f::1/128`, use the commands:

```
awplus# configure terminal
awplus(config)# no ipv6 access-list extended ACL-1 deny proto
10 2001:0db8:1::1/128 2001:0db8:f::1/128
```

Related Commands

ipv6 access-list extended (named)

(ipv6 access-list extended IP protocol filter)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

(ipv6 access-list extended IP protocol filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol specified, to the current extended IPv6 access-list. If a sequence is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with or without an IP protocol filter entry, from the current extended IPv6 access-list. You can specify the ACL filter entry by entering either its sequence number, or its filter entry profile.

Syntax [ip|proto]

```
[<sequence-number>] {deny|permit} {ip|any|proto <ip-protocol>}
{<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]

no {deny|permit} {ip|any|proto <ip-protocol>}
{<ipv6-source-address/prefix>|any}
{<ipv6-destination-address/prefix>|any} [log]

no [<sequence-number>]
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
ip	IP packet.
any	Any packet.
proto *<ip-protocol>*	<1-255> Specify IP protocol number, as defined by IANA (Internet Assigned Numbers Authority www.iana.org/assignments/protocol-numbers) See below for a list of IP protocol numbers and their descriptions.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
<ipv6- destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any destination address or remote address.
log	Log the results.

Table 27-3: IP protocol number and description

Protocol Number	Protocol Description [RFC]
1	Internet Control Message [RFC792]
2	Internet Group Management [RFC1112]
3	Gateway-to-Gateway [RFC823]
4	IP in IP [RFC2003]
5	Stream [RFC1190] [RFC1819]
6	TCP (Transmission Control Protocol) [RFC793]
8	EGP (Exterior Gateway Protocol) [RFC888]
9	IGP (Interior Gateway Protocol) [IANA]
11	Network Voice Protocol [RFC741]
17	UDP (User Datagram Protocol) [RFC768]
20	Host monitoring [RFC869]
27	RDP (Reliable Data Protocol) [RFC908]
28	IRTP (Internet Reliable Transaction Protocol) [RFC938]
29	ISO-TP4 (ISO Transport Protocol Class 4) [RFC905]
30	Bulk Data Transfer Protocol [RFC969]
33	DCCP (Datagram Congestion Control Protocol) [RFC4340]
48	DSR (Dynamic Source Routing Protocol) [RFC4728]
50	ESP (Encap Security Payload) [RFC2406]
51	AH (Authentication Header) [RFC2402]
54	NARP (NBMA Address Resolution Protocol) [RFC1735]
58	ICMP for IPv6 [RFC1883]
59	No Next Header for IPv6 [RFC1883]
60	Destination Options for IPv6 [RFC1883]
88	EIGRP (Enhanced Interior Gateway Routing Protocol)
89	OSPFIGP [RFC1583]
97	Ethernet-within-IP Encapsulation / RFC3378
98	Encapsulation Header / RFC1241
108	IP Payload Compression Protocol / RFC2393
112	Virtual Router Redundancy Protocol / RFC3768
134	RSVP-E2E-IGNORE / RFC3175
135	Mobility Header / RFC3775
136	UDPLite / RFC3828

Table 27-3: IP protocol number and description (cont.)

Protocol Number	Protocol Description [RFC]
137	MPLS-in-IP / RFC4023
138	MANET Protocols / RFC-ietf-manet-iana-07.txt
139-252	Unassigned / IANA
253	Use for experimentation and testing / RFC3692
254	Use for experimentation and testing / RFC3692
255	Reserved / IANA

Mode IPv6 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any IP protocol type packet that has the specified source and destination IPv6 addresses and the specified IP protocol type. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add a new ACL filter entry to the extended IPv6 access-list named `my-list` with sequence number `5` rejecting the IPv6 packet from `2001:db8:1:1` to `2001:db8:f:1`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny ip 2001:db8:1::1/128
2001:db8:f::1/128
```

To remove the ACL filter entry to the extended IPv6 access-list named `my-list` with sequence number `5`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# no 5
```

Related Commands

ipv6 access-list extended (named)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

(ipv6 access-list extended TCP UDP filter)

Overview

Use this ACL filter to add a filter entry for an IPv6 source and destination address and prefix, with a TCP (Transmission Control Protocol) or UDP (User Datagram Protocol) source and destination port specified, to the current extended IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source and destination address and prefix, with a TCP or UDP source and destination port specified, from the current extended IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax [tcp|udp]

```
[<sequence-number>] {deny|permit} {tcp|udp}
{<ipv6-source-address/prefix>|any} {eq <sourceport>|lt
<sourceport>|gt <sourceport>|ne <sourceport>}
{<IPv6-destination-address/prefix>|any} {eq <destport>|lt
<destport>|gt <destport>|ne <destport>} [log]
```

```
no {deny|permit} {tcp|udp} {<ipv6-source-address/prefix>|any}
{eq <sourceport>|lt <sourceport>|gt <sourceport>|ne
<sourceport>}} {<IPv6-destination-address/prefix>|any} {eq
<destport>|lt <destport>|gt <destport>|ne <destport>} [log]
```

```
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
tcp	TCP packet.
udp	UDP packet.
<ipv6-source-address/prefix>	IPv6 source address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
any	Any source address or local address.
eq	Equal to.
lt	Less than.
gt	Greater than.
ne	Not equal to.
<sourceport>	The source port number, specified as an integer between 0 and 65535.

Parameter	Description
<ipv6-destination-address/prefix>	IPv6 destination address, or local address. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<destport>	The destination port number, specified as an integer between 0 and 65535.
`log`	Log the results.

Mode IPv6 Extended ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any packet that has the specified source and destination IPv6 addresses and the specified TCP or UDP source and destination port. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add a new filter entry with sequence number `5` to the access-list named `my-list` to reject TCP packets from 2001:0db8::0/64 port `10` to 2001:0db8::f/64 port `20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny tcp 2001:0db8::0/64 eq 10
2001:0db8::f/64 eq 20
```

To add a new filter entry with sequence number `5` to the extended IPv6 access-list named `my-list` to reject UDP packets from 2001:0db8::0/64 port `10` to 2001:0db8::f/ 64 port `20`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# 5 deny udp 2001:0db8::0/64 eq 10
2001:0db8::f/64 eq 20
```

To remove the filter entry with sequence number `5`to the extended IPv6 access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list extended my-list
awplus(config-ipv6-ext-acl)# no 5
```

Related Commands ipv6 access-list extended (named)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

ipv6 access-list standard (named)

Overview This command configures an IPv6 standard access-list for filtering frames that permit or deny IPv6 packets from a specific source IPv6 address.

The **no** variant of this command removes a specified IPv6 standard access-list.

Syntax [list-name]

```
ipv6 access-list standard <ipv6-acl-list-name>
no ipv6 access-list standard <ipv6-acl-list-name>
```

Parameter	Description
<ipv6-acl-list-name>	A user-defined name for the IPv6 software standard access-list.

Syntax [deny|permit]

```
ipv6 access-list standard <ipv6-acl-list-name> [{deny|permit}
{<ipv6-source-address/prefix-length>|any} [exact-match]]
no ipv6 access-list standard <ipv6-acl-list-name>
[{deny|permit} {<ipv6-source-address/prefix-length>|any}
[exact-match]]
```

Parameter	Description
<ipv6-acl-list-name>	A user-defined name for the IPv6 software standard access-list.
`deny`	The IPv6 software standard access-list rejects packets that match the type, source, and destination filtering specified with this command.
`permit`	The IPv6 software standard access-list permits packets that match the type, source, and destination filtering specified with this command.
<ipv6-source-address/prefix-length>	Specifies a source address and prefix length. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64.
`any`	Matches any source IPv6 address.
`exact-match`	Exact match of the prefixes.

Mode Global Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage Use IPv6 standard access-lists to control the transmission of IPv6 packets on an interface, and restrict the content of routing updates. The switch stops checking the IPv6 standard access-list when a match is encountered.

For backwards compatibility you can either create IPv6 standard access-lists from within this command, or you can enter `ipv6 access-list standard` followed by only the IPv6 standard access-list name. This latter (and preferred) method moves you to the `(config-ipv6-std-acl)` prompt for the selected IPv6 standard access-list, and from here you can configure the filters for this selected IPv6 standard access-list.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Example To enter the IPv6 Standard ACL Configuration mode for the access-list named `my-list`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)#
```

Related Commands

(ipv6 access-list standard filter)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

(ipv6 access-list standard filter)

Overview Use this ACL filter to add a filter entry for an IPv6 source address and prefix length to the current standard IPv6 access-list. If a sequence number is specified, the new entry is inserted at the specified location. Otherwise, the new entry is added at the end of the access-list.

The **no** variant of this command removes a filter entry for an IPv6 source address and prefix from the current standard IPv6 access-list. You can specify the filter entry for removal by entering either its sequence number, or its filter entry profile.

Syntax [icmp]

```
[<sequence-number>] {deny|permit}
{<ipv6-source-address/prefix-length>|any}
no {deny|permit} {<ipv6-source-address/prefix-length>|any}
no <sequence-number>
```

Parameter	Description
<sequence-number>	<1-65535> The sequence number for the filter entry of the selected access control list.
deny	Specifies the packets to reject.
permit	Specifies the packets to accept.
<ipv6-source-address/prefix-length>	IPv6 source address and prefix-length in the form X:X::X:X/P.
any	Any IPv6 source host address.

Mode IPv6 Standard ACL Configuration

Default Any traffic controlled by a software ACL that does not explicitly match a filter is denied.

Usage The filter entry will match on any IPv6 packet that has the specified IPv6 source address and prefix length. The parameter `any` may be specified if an address does not matter.

NOTE: *Software ACLs will **deny** access unless **explicitly permitted** by an ACL action.*

Examples To add an ACL filter entry with sequence number `5` that will deny any IPv6 packets to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# 5 deny any
```

To remove the ACL filter entry that will deny any IPv6 packets from the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no deny any
```

Alternately, to remove the ACL filter entry with sequence number `5` to the standard IPv6 access-list named `my-list`, enter the commands:

```
awplus# configure terminal
awplus(config)# ipv6 access-list standard my-list
awplus(config-ipv6-std-acl)# no 5
```

Related Commands

ipv6 access-list standard (named)

show ipv6 access-list (IPv6 Software ACLs)

show running-config

show ipv6 access-list (IPv6 Software ACLs)

Overview Use this command to display all configured IPv6 access-lists or the IPv6 access-list specified by name.

Syntax

```
show ipv6 access-list [<access-list-name>]
show ipv6 access-list standard [<access-list-name>]
show ipv6 access-list extended [<access-list-name>]
```

Parameter	Description
<access-list-name>	Only display information about an IPv6 access-list with the specified name.
`standard`	Only display information about standard access-lists.
`extended`	Only display information about extended access-lists.

Mode User Exec and Privileged Exec

Example To show all configured IPv6 access-lists, use the following command:

```
awplus# show ipv6 access-list
```

Output Figure 27-1: Example output from **show ipv6 access-list**

```
IPv6 access-list deny_icmp
  deny icmp any any vlan 1

IPv6 access-list deny_ssh
  deny tcp abcd::0/64 any eq 22
```

Example To show the IPv6 access-list named **deny_icmp,** use the following command:

```
awplus# show ipv6 access-list deny_icmp
```

Output Figure 27-2: Example output from **show ipv6 access-list** for a named ACL

```
IPv6 access-list deny_icmp
  deny icmp any any vlan 1
```

Related Commands

ipv6 access-list extended (named)

(ipv6 access-list extended IP protocol filter)

ipv6 access-list standard (named)

(ipv6 access-list extended TCP UDP filter)

(ipv6 access-list standard filter)

vty ipv6 access-class (named)

Overview For IPv6, use this command to set a standard named software access list to be the management ACL. This is then applied to all available VTY lines for controlling remote access by Telnet and SSH. This command allows or denies packets containing the IPv6 addresses included in the ACL to create a connection to your device.

ACLs that are attached using this command have an implicit 'deny-all' filter as the final entry in the ACL. A typical configuration is to permit a specific address, or range of addresses, and rely on the 'deny-all' filter to block all other access.

Use the **no** variant of this command to remove the access list.

Syntax

```
vty ipv6 access-class <access-name>
no vty ipv6 access-class [<access-name>]
```

Parameter	Description
<access-name>	Specify an IPv6 standard software access-list name

Mode Global Configuration

Examples To set the named standard access-list named **access-ctrl** to be the IPv6 management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# vty ipv6 access-class access-ctrl
```

To remove **access-ctrl** from the management ACL, use the following commands:

```
awplus# configure terminal
awplus(config)# no vty ipv6 access-class access-ctrl
```

Output Figure 27-3: Example output from the **show running-config** command

```
awplus#showrunning-config|grep access-class

vty ipv6 access-class access-ctrl
```

Related Commands

show running-config

vty access-class (numbered)

28 QoS Commands

Introduction

Overview This chapter provides an alphabetical reference for Quality of Service commands.

QoS uses ACLs. For more information about ACLs, see the ACL Feature Overview and Configuration Guide.

Command List

class

Overview Use this command to associate an existing class-map to a policy or policy-map (traffic classification), and to enter Policy Map Class Configuration mode to configure the class- map.

Use the **no** variant of this command to delete an existing class-map.

If your class-map does not exist, you can create it by using the class-map command.

Syntax

```
class {<name>|default}
no class <name>
```

Parameter	Description
<name>	Name of the (already existing) class-map.
`default`	Specify the default class-map.

Mode Policy Map Configuration

Example The following example creates the policy-map `pmap1`(using the policy-map command), then associates this to an already existing class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)#
```

Related Commands class-map

policy-map

class-map

Overview Use this command to create a class-map.

Use the **no** variant of this command to delete the named class-map.

Syntax

```
class-map <name>
no class-map <name>
```

Parameter	Description
<name>	Name of the class-map to be created.

Mode Global Configuration

Example This example creates a class-map called `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)#
```

clear mls qos interface policer-counters

Overview Resets an interface's policer counters to zero. You can either clear a specific class-map, or you can clear all class-maps by not specifying a class map.

Syntax
```
clear mls qos interface <port> policer-counters [class-map
<class-map>]
```

Parameter	Description
<port>	The port may be a switch port (e.g. `port1.0.4`), a static channel group (e.g. `sa3`), or a dynamic (LACP) channel group (e.g. `po4`).
`class-map`	Select a class-map.
<class-map>	Class-map name.

Mode Privileged Exec

Example To reset the policy counters to zero for all class-maps for `port1.0.1`, use the command:

```
awplus# clear mls qos interface port1.0.1 policer-counters
```

Related Commands show mls qos interface policer-counters

default-action

Overview Sets the action for the default class-map belonging to a particular policy-map. The action for a non-default class-map depends on the action of any ACL that is applied to the policy-map.

The default action can therefore be thought of as specifying the action that will be applied to any data that does not meet the criteria specified by the applied matching commands.

Use the **no** variant of this command to reset to the default action of 'permit'.

Syntax

```
default-action
[permit|deny|send-to-cpu|copy-to-cpu|copy-to-mirror|
send-to-mirror]
```

```
no default-action
```

Parameter	Description
`permit`	Packets to permit.
`deny`	Packets to deny.
`send-to-cpu`	Specify packets to send to the CPU.
`copy-to-cpu`	Specify packets to copy to the CPU.
`copy-to-mirror`	Specify packets to copy to the mirror port.
`send-to-mirror`	Specify packets to send to the mirror port.

Default The default is '`permit`'.

Mode Policy Map Configuration

Examples To set the action for the default class-map to `deny`, use the command:

```
awplus(config-pmap)# default-action deny
```

To set the action for the default class-map to `copy-to-mirror` for use with the mirror interface command, use the command:

```
awplus(config-pmap)# default-action copy-to-mirror
```

Related Commands mirror interface

description (QoS policy-map)

Overview Adds a textual description of the policy-map. This can be up to 80 characters long.

Use the **no** variant of this command to remove the current description from the policy-map.

Syntax

```
description <line>
no description
```

Parameter	Description
<line>	Up to 80 character long line description.

Mode Policy Map Configuration

Example To add the description, VOIP traffic, use the command:

```
awplus(config-pmap)# description VOIP traffic
```

egress-rate-limit

Overview Use this command to limit the amount of traffic that can be transmitted per second from this port.

Use the **no** variant of this command to disable the limiting of traffic egressing on the interface.

Syntax

```
egress-rate-limit <bandwidth>
no egress-rate-limit
```

Parameter	Description
<bandwidth>	Bandwidth <1-10000000 units per second> (usable units: k, m, g). The egress rate limit can be configured in multiples of 64kbps. If you configure a value that is not an exact multiple of 64kbps, then the value will be rounded up to the nearest higher exact multiple of 64kbps. The minimum is 64 Kb. The default unit is Kb (**k**), but Mb (**m**) or Gb (**g**) can also be specified. The command syntax is not case sensitive, so a value such as 20m or 20M will be interpreted as 20 megabits.

Mode Interface Configuration

Examples To enable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# egress-rate-limit 64k
% Egress rate limit has been set to 64 Kb
```

To disable egress rate limiting on a port, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no egress-rate-limit
```

match access-group

Overview Use this command to define match criterion for a class-map.

Syntax

```
match access-group {<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}
no match access-group
{<hw-IP-ACL>|<hw-MAC-ACL>|<hw-named-ACL>}
```

Parameter	Description
<hw-IP-ACL>	Specify a hardware IP ACL number in the range <3000-3699>.
<hw-MAC-ACL>	Specify a hardware MAC ACL number in the range <4000-4699>.
<hw-named-ACL>	Specify the hardware named ACL.

Mode Class Map Configuration

Usage First create an access-list that applies the appropriate permit/deny requirements. Then use the **match access-group** command to apply this access-list for matching to a class-map. Note that this command will apply the access-list matching only to *incoming* data packets.

Examples To configure a class-map named `cmap1` with one match criterion: `access-list 3001`, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 3001 permit ip any any
awplus(config)# class-map cmap1
awplus(config-cmap)# match access-group 3001
```

To configure a class-map named `cmap2` with one match criterion: `access-list 3001`, which allows MAC traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list 4001 permit any any
awplus(config)# class-map cmap2
awplus(config-cmap)# match access-group 4001
```

To configure a class-map named `cmap3` with one match criterion: `access-list hw_acl`, which allows IP traffic from any source to any destination, use the commands:

```
awplus# configure terminal
awplus(config)# access-list hardware hw_acl
awplus(config-ip-hw-acl)# permit ip any any
awplus(config)# class-map cmap3
awplus(config-cmap)# match access-group hw_acl
```

Related Commands class-map

match cos

Overview Use this command to define a COS to match against incoming packets.

Use the **no** variant of this command to remove CoS.

Syntax

```
match cos <0-7>
no match cos
```

Parameter	Description
<0-7>	Specify the CoS value.

Mode Class Map Configuration

Examples To set the class-map's CoS to 4, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match cos 4
```

To remove CoS from a class-map, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match cos
```

match dscp

Overview Use this command to define the DSCP to match against incoming packets.

Use the **no** variant of this command to remove a previously defined DSCP.

Syntax

```
match dscp <0-63>
no match dscp
```

Parameter	Description
<0-63>	Specify DSCP value (only one value can be specified).

Mode Class Map Configuration

Usage Use the **match dscp** command to define the match criterion after creating a class-map.

Examples To configure a class-map named `cmap1` with criterion that matches DSCP 56, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match dscp 56
```

To remove a previously defined DSCP from a class-map named cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match dscp
```

Related Commands class-map

match eth-format protocol

Overview This command sets the Ethernet format and the protocol for a class-map to match on.

Select one Layer 2 format and one Layer 3 protocol when you issue this command.

Use the **no** variant of this command to remove the configured Ethernet format and protocol from a class-map.

Syntax

```
match eth-format <layer-two-format> protocol
<layer-three-protocol>
```

```
no match eth-format protocol
```

Parameter	Description
<layer-two-formats>	
802dot2-tagged	802.2 Tagged Packets (enter the parameter name).
802dot2-untagged	802.2 Untagged Packets (enter the parameter name).
ethii-tagged	EthII Tagged Packets (enter the parameter name).
ethii-untagged	EthII Untagged Packets (enter the parameter name).
ethii-any	EthII Tagged or Untagged Packets (enter the parameter name).
netwareraw-tagged	Netware Raw Tagged Packets (enter the parameter name).
netwareraw-untagged	Netware Raw Untagged Packets (enter the parameter name).
snap-tagged	SNAP Tagged Packets (enter the parameter name).
snap-untagged	SNAP Untagged Packets (enter the parameter name).
<layer-three-protocols>	
<word>	A Valid Protocol Number in hexidecimal.
any	Note that the parameter “any” is only valid when used with the netwarerawtagged and netwarerawuntagged protocol options.
sna-path-control	Protocol Number 04 (enter the parameter name or its number).
proway-lan	Protocol Number 0E (enter the parameter name or its number).
eia-rs Protocol	Number 4E (enter the parameter name or its number).
proway Protocol	Number 8E (enter the parameter name or its number).
ipx-802dot2	Protocol Number E0 (enter the parameter name or its number).

Parameter	Description
netbeui	Protocol Number F0 (enter the parameter name or its number).
iso-clns-is	Protocol Number FE (enter the parameter name or its number).
xdot75-internet	Protocol Number 0801(enter the parameter name or its number).
nbs-internet	Protocol Number 0802 (enter the parameter name or its number).
ecma-internet	Protocol Number 0803 (enter the parameter name or its number).
chaosnet	Protocol Number 0804 (enter the parameter name or its number).
xdot25-level-3	Protocol Number 0805 (enter the parameter name or its number).
arp Protocol	Number 0806 (enter the parameter name or its number).
xns-compat	Protocol Number 0807 (enter the parameter name or its number).
banyan-systems	Protocol Number 0BAD (enter the parameter name or its number).
bbn-simnet	Protocol Number 5208 (enter the parameter name or its number).
dec-mop-dump-ld	Protocol Number 6001 (enter the parameter name or its number).
dec-mop-rem-cdons	Protocol Number 6002 (enter the parameter name or its number).
dec-decnet	Protocol Number 6003 (enter the parameter name or its number).
dec-lat	Protocol Number 6004 (enter the parameter name or its number).
dec-diagnostic	Protocol Number 6005 (enter the parameter name or its number).
dec-customer	Protocol Number 6006 (enter the parameter name or its number).
dec-lavc	Protocol Number 6007 (enter the parameter name or its number).
rarp	Protocol Number 8035 (enter the parameter name or its number).
dec-lanbridge	Protocol Number 8038 (enter the parameter name or its number).
dec-encryption	Protocol Number 803D (enter the parameter name or its number).

Parameter	Description
appletalk	Protocol Number 809B (enter the parameter name or its number).
ibm-sna	Protocol Number 80D5 (enter the parameter name or its number).
appletalk-aarp	Protocol Number 80F3 (enter the parameter name or its number).
snmp	Protocol Number 814CV.
ethertalk-2	Protocol Number 809B (enter the parameter name or its number).
ethertalk-2-aarp	Protocol Number 80F3 (enter the parameter name or its number).
ipx-snap	Protocol Number 8137 (enter the parameter name or its number).
ipx-802dot3	Protocol Number FFFF (enter the parameter name or its number).
ip	Protocol Number 0800 (enter the parameter name or its number).
ipx	Protocol Number 8137 (enter the parameter name or its number).
ipv6	Protocol Number 86DD (enter the parameter name or its number).

Mode Class Map Configuration

Examples To set the eth-format to ethii-tagged and the protocol to 0800 (IP) for class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match eth-format ethii-tagged protocol
0800
awplus#
awplus(config-cmap)# match eth-format ethii-tagged protocol ip
```

To remove the eth-format and the protocol from the class-map cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match eth-format protocol
```

match inner-cos

Overview Sets the Inner CoS for a class-map to match on.

Use the **no** variant of this command to remove CoS.

Syntax

```
match inner-cos <0-7>
no match inner-cos
```

Parameter	Description
<0-7>	Specify the Inner CoS value.

Mode Class Map Configuration

Examples To set the class-map's inner-cos to 4, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match inner-cos 4
```

To remove CoS from the class-map, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match inner-cos
```

match inner-vlan

Overview Use this command to define the inner VLAN ID as match criteria.

Use the **no** variant of this command to disable the VLAN ID used as match criteria.

Syntax

```
match inner-vlan <1-4094>
no match inner-vlan
```

Parameter	Description
<1-4094>	The VLAN number.

Mode Class Map Configuration

Usage This command is used in double-tagged networks to match on a VLAN ID belonging to the client network. For more information on VLAN double-tagged networks, see the VLAN Feature Overview and Configuration Guide.

Examples To configure a class-map named `cmap1` to match traffic from inner VLAN 3, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match inner-vlan 3
```

To disable the configured VLAN ID as a match criteria for the class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match inner-vlan
```

match ip-precedence

Overview Use this command to identify IP precedence values as match criteria.

Use the **no** variant of this command to remove IP precedence values from a class-map.

Syntax

```
match ip-precedence <0-7>
no match ip-precedence
```

Parameter	Description
<0-7>	The precedence value to be matched.

Mode Class Map Configuration

Example To configure a class-map named `cmap1` to match all IPv4 packets with a precedence value of `5`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match ip-precedence 5
```

match mac-type

Overview Use this command to set the MAC type for a class-map to match on.

Use **no** variant of this command to remove the MAC type match entry.

Syntax

```
match mac-type {l2bcast|l2mcast|l2ucast}
no match mac-type
```

Parameter	Description
l2bcast	Layer 2 Broadcast traffic.
l2mcast	Layer 2 Multicast traffic.
l2ucast	Layer 2 Unicast traffic.

Mode Class Map Configuration

Examples To set the class-map's MAC type to Layer 2 multicast, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match mac-type l2mcast
```

To remove the class-map's MAC type entry, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match mac-type
```

match tcp-flags

Overview Sets one or more TCP flags (control bits) for a class-map to match on.

Use the **no** variant of this command to remove one or more TCP flags for a class-map to match on.

Syntax

```
match tcp-flags {[ack][fin][psh][rst][syn][urg]}
no match tcp-flags {[ack][fin][rst][syn][urg]}
```

Parameter	Description
ack	Acknowledge.
fin	Finish.
psh	Push
rst	Reset.
syn	Synchronize.
urg	Urgent.

Mode Class Map Configuration

Examples To set the class-map's TCP flags to `ack` and `syn`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# match tcp-flags ack syn
```

To remove the TCP flags `ack` and `rst`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map
awplus(config-cmap)# no match tcp-flags ack rst
```

match vlan

Overview Use this command to define the VLAN ID as match criteria.

Use the **no** variant of this command to disable the VLAN ID used as match criteria.

Syntax

```
match vlan <1-4094>
no match vlan
```

Parameter	Description
<1-4094>	The VLAN number.

Mode Class Map Configuration

Examples To configure a class-map named `cmap1` to include traffic from VLAN 3, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# match vlan 3
```

To disable the configured VLAN ID as a match criteria for the class-map named `cmap1`, use the commands:

```
awplus# configure terminal
awplus(config)# class-map cmap1
awplus(config-cmap)# no match vlan
```

mls qos cos

Overview This command assigns a CoS (Class of Service) user-priority value to untagged frames entering a specified interface. By default, all untagged frames are assigned a CoS value of 0.

Use the **no** variant of this command to return the interface to the default CoS setting for untagged frames entering the interface.

Syntax

```
mls qos cos <0-7>
no mls qos cos
```

Parameter	Description
<0-7>	The Class of Service, user-priority value.

Default By default, all untagged frames are assigned a CoS value of 0. Note that for tagged frames, the default behavior is not to alter the CoS value.

Mode Interface Configuration

Example To assign a CoS user priority value of 2 to all untagged packets entering ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# mls qos cos 2
```

mls qos enable

Overview Use this command to globally enable QoS on the switch or stack.

Use the **no** variant of this command to globally disable QoS and remove all QoS configuration. The **no** variant of this command removes all class-maps, policy-maps, and policers that have been created. Running the **no mls qos** command will therefore remove all pre-existing QoS configurations on the switch.

Mode Global Configuration

Syntax

```
mls qos enable
no mls qos
```

Example To enable QoS on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# mls qos enable
```

mls qos map cos-queue to

Overview Use this command to set the default CoS to egress queue mapping. This is the default queue mapping for packets that do not get assigned an egress queue via any other QoS functionality.

Use the **no** variant of this command to reset the cos-queue map back to its default setting. The default mappings for this command are:

```
    CoS Priority :      0 1 2 3 4 5 6 7
    --------------------------------

  CoS QUEUE:          2 0 1 3 4 5 6 7
```

Syntax

```
mls qos map cos-queue <cos-priority> to <queue-number>
no mls qos map cos-queue
```

Parameter	Description
<cos-priority>	CoS priority value. Can take a value between 0 and 7.
<queue-number>	Queue number. Can take a value between 0 and 7.

Mode Global Configuration

Examples To map CoS 2 to queue 0, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map cos-queue 2 to 0
```

To set the cos-queue map back to its defaults, use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map cos-queue
```

Related Commands show mls qos interface

mls qos map premark-dscp to

Overview This command configures the premark-dscp map. It is used when traffic is classified by a class-map that has trust dscp configured. Based on a lookup DSCP, the map determines new QoS settings for the traffic.

The **no** variant of this command resets the premark-dscp map to its defaults. If no DSCP is specified then all DSCP entries will be reset to their defaults.

Syntax

```
mls qos map premark-dscp <0-63> to
{[new-dscp <0-63>][new-cos <0-7>]
[new-bandwidth-class {green|yellow|red}]}

no mls qos map premark-dscp [<0-63>]
```

Parameter	Description
`premark-dscp <0-63>`	The DSCP value on ingress.
`new-dscp <0-63>`	The DSCP value that the packet will have on egress. If unspecified, this value will remain the DSCP ingress value.
`new-cos <0-7>`	The CoS value that the packet will have on egress. If unspecified, this value will retain its value on ingress.
`new-bandwidth-class`	Modify Egress Bandwidth-class. If unspecified, this value will be set to green.
`green`	Egress Bandwidth-class green (marked down Bandwidth-class).
`yellow`	Egress Bandwidth-class yellow (marked down Bandwidth-class).
`red`	Egress Bandwidth-class red (marked down Bandwidth-class).

Mode Global Configuration

Usage With the trust dscp command set, this command (**mls qos map premark-dscp**) enables you to make the following changes:

- remap the DSCP (leaving the other settings unchanged)
- remap any or all of CoS, output queue, or bandwidth class values (leaving the DSCP unchanged)

NOTE:

If you attempt to remap both the DSCP and another setting, only the DSCP remap will take effect.

Example To set the entry for DSCP 1 to use a new DSCP of 2, a new CoS of 3, and a new bandwidth class of yellow, use the command:

```
awplus# configure terminal
awplus(config)# mls qos map premark-dscp 1 to new-dscp 2 new-cos
3 new-bandwidth-class yellow
```

Example To reset the entry for DSCP 1 use the command:

```
awplus# configure terminal
awplus(config)# no mls qos map premark-dscp 1
```

Related Commands show mls qos maps premark-dscp

trust dscp

no police

Overview Use this command to disable any policer previously configured on the class-map.

Syntax

```
no police
```

Mode Policy Map Class Configuration

Usage This command disables any policer previously configured on the class-map.

Example To disable policing on a class-map use the command:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# no police
```

police single-rate action

Overview Configures a single-rate policer for a class-map.

Syntax

```
police single-rate <cir> <cbs> <ebs> action
{drop-red|remark-transmit}
```

Parameter	Description	
<cir>	Specify the Committed Information Rate (CIR) (1-40000000 kbps).	
<cbs>	Specify the Committed Burst Size (CBS) (0-16777216 bytes).	
<ebs>	Specify a Excess Burst Size (EBS) (0-16777216 bytes).	
`action`	Specify the action if the rate is exceeded.	
	`drop-red`	Drop the red packets.
	`remark-transmit`	Modify the packets using the remark map, then transmit. You can configure the remark map using the remark-map command.

Mode Policy Map Class Configuration

Usage You can use a policer to meter the traffic classified by the class-map and assign it to one of three bandwidth classes.

The bandwidth classes are green (conforming), yellow (partially-conforming), and red (non-conforming). A single-rate policer is based on three values. These are the average rate, minimum burst and maximum burst.

Color	Definition
`green`	The traffic rate is less than the average rate and minimum burst.
`yellow`	The traffic rate is between the minimum burst and the maximum burst.
`red`	The traffic rate exceeds the average rate and the maximum burst.

Using an action of drop-red means that any packets classed as red are discarded.

NOTE: *This command will not take effect when applied to a class-map that attaches to a channel group whose ports span processor instances.*

Note that the remark-map does not only apply to red traffic. If a remark-map is configured on the same class-map as the policer, then the remark-map will apply to green- colored and yellow-colored traffic irrespective of the value configured on the **action** parameter of the policer. So, even if **action** is configured to **drop-red,** the remark-map will be applied to green and yellow traffic. So, the **action** parameter only applies to red- colored traffic. If **action** is set to **drop-red**, then red

traffic is dropped; if **action** is set to **remark-transmit**, then the red traffic has the action of the remark map applied to it, and is then transmitted.

Example To configure a single rate meter measuring traffic of 10 Mbps that drops a sustained burst of traffic over this rate, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police single-rate 10000 1875000 1875000
action drop-red
```

Related Commands

no police

police twin-rate action

remark-map

police twin-rate action

Overview Configures a twin-rate policer for a class-map.

Syntax

```
police twin-rate <cir> <pir> <cbs> <pbs> action
{drop-red|remark-transmit}
```

Parameter	Description	
<cir>	Specify the Committed Information Rate (CIR) (1-40000000 kbps).	
<pir>	Specify the Peak Information Rate (PIR) (1-40000000 kbps).	
<cbs>	Specify the Committed Burst Size (CBS) (0-16777216 bytes).	
<pbs>	Specify the Peak Burst Size (PBS) (0-16777216 bytes).	
`action`	Specify the action if rate is exceeded.	
	`drop-red`	Drop the red packets.
	`remark-transmit`	Modify the packets using the remark map, then transmit. You can configure the remark map using the remark-map command.

Mode Policy Map Class Configuration

Usage A policer can be used to meter the traffic classified by the class-map and as a result will be given one of three bandwidth classes. These are green (conforming), yellow (partially- conforming), and red (non-conforming).

A twin-rate policer is based on four values. These are the minimum rate, minimum burst size, maximum rate, and maximum burst size.

Bandwidth Class	Definition
`green`	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that is less than that set for the CBS.
`yellow`	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time results in a value that is between those set for the CBS and the PBS.
`red`	The sum of the number of existing (buffered) bytes plus those arriving at the port per unit time, result in a value that exceeds that set for the PBS.

Using an action of drop-red means that any packets classed as red will be discarded.

Using an action of remark-transmit means that the packet will be remarked with the values configured in the policed-dscp map. The index into this map is determined by the DSCP in the packet.

Note that the remark-map does not only apply to red traffic. If a remark-map is configured on the same class-map as the policer, then the remark-map will apply to green- colored and yellow-colored traffic irrespective of the value configured on the **action** parameter of the policer. So, even if **action** is configured to **drop-red,** the remark-map will be applied to green and yellow traffic. So, the **action** parameter only applies to red- colored traffic. If **action** is set to **drop-red**, then red traffic is dropped; if **action** is set to **remark-transmit**, then the red traffic has the action of the remark map applied to it, and is then transmitted.

Example To configure a twin rate meter measuring a minimum rate of 10 Mbps and a maximum rate of 20 Mbps that uses the premark map to remark any non-conforming traffic, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map name
awplus(config-pmap)# class classname
awplus(config-pmap-c)# police twin-rate 10000 20000 1875000
3750000 action remark-transmit
```

Related Commands

no police

police single-rate action

policy-map

Overview Use this command to create a policy-map and to enter Policy Map Configuration mode to configure the specified policy-map.

Use the **no** variant of this command to delete an existing policy-map.

Syntax

```
policy-map <name>
no policy-map <name>
```

Parameter	Description
<name>	Name of the policy-map.

Mode Global Configuration

Example To create a policy-map called pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)#
```

Related Commands class-map

priority-queue

Overview Configures strict priority based scheduling on the specified egress queues. You must specify at least one queue.

Syntax

```
priority-queue [0][1][2][3][4][5][6][7]
```

Parameter	Description
`[0][1]...[7]`	Specify the queues that will use strict priority scheduling. With strict priority scheduling, the switch will completely empty the highest numbered queue first, then start processing the next lowest numbered queue.

Mode Interface Configuration.

Usage By default, the queues on all ports are set for priority queuing. You can change the queue emptying sequence to weighted round robin, by using the wrr-queue weight queues command. You can then use the priority-queue command to reset the selected queues to priority queuing.

Note that the emptying sequence for priority queuing is always highest queue number to lowest queue number.

Example To apply priority based scheduling to egress queues 1 and 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# priority-queue 1 2
```

Related Commands

show mls qos interface

show mls qos interface queue-counters

wrr-queue weight queues

remark-map

Overview Use this command to configure the remark map. If a re-mark map is applied to a class, and a policer is also applied to the same class, then:

- green and yellow traffic will all be acted upon by the remark-map, and
- red traffic will be either dropped or acted upon by the remark-map, depending on whether the policer **action** is set to **drop-red** or **remark-transmit**.

The **no** variant of this command resets the remark map to its defaults. Specifying the bandwidth class is optional. If no bandwidth class is specified, then all bandwidth classes are reset to their defaults.

Syntax

```
remark-map [bandwidth-class {green|yellow|red}] to {[new-dscp <0-63>] [new-bandwidth-class {green|yellow|red}]}
```

```
no remark-map [bandwidth-class {green|yellow|red}] to {[new-dscp <0-63>] [new-bandwidth-class {green|yellow|red}]}
```

Parameter	Description
`bandwidth-class`	Specify the bandwidth class of packets to remark.
`green`	Remark green packets.
`yellow`	Remark yellow packets.
`red`	Remark red packets.
`new-dscp`	Specify the new DSCP value.
<0-63>	The DSCP value.
`new-bandwidth-class`	Specify the new bandwidth class.
`green`	Remark the packet green.
`yellow`	Remark the packet yellow.
`red`	Remark the packet red.

Mode Policy Map Class Configuration

Examples To remark the policed green traffic to a new DSCP of `2` and a new bandwidth class of `yellow`, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class green to new-dscp 2 new-bandwidth-class yellow
```

To remark the policed green traffic to a new DSCP of 2, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark-map bandwidth-class green to
new-dscp 2
```

To reset the DSCP for all bandwidth classes, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# no remark-map to new-dscp
```

Related Commands

police single-rate action

police twin-rate action

remark new-cos

Overview This command enables you to configure and remark either or both of:

- the CoS flag in the data packet
- the input into the CoS to queue map, thus changing the destination egress queue.

Syntax

```
remark new-cos <0-7> [internal|external|both]
no remark new-cos [internal|external|both]
```

Parameter	Description
`<0-7>`	The new value for the CoS flag and/or the input into the CoS to queue map.
`external`	Remarks the CoS flag in the packet.
`internal`	Remarks the new-CoS input into the CoS to queue map.
`both`	Remarks (with the same value) both the CoS flag in the packet and the input to the CoS to queue map.

Mode Policy Map Class Configuration

Usage The default CoS to Queue mappings are shown in the following table:

CoS Value	0	1	2	3	4	5	6	7
Egress Queue No	2	0	1	3	4	5	6	7

The relationship between this command and the CoS to queue map is shown in the following figure.

Figure 28-1: Remarking and the CoS to Q map

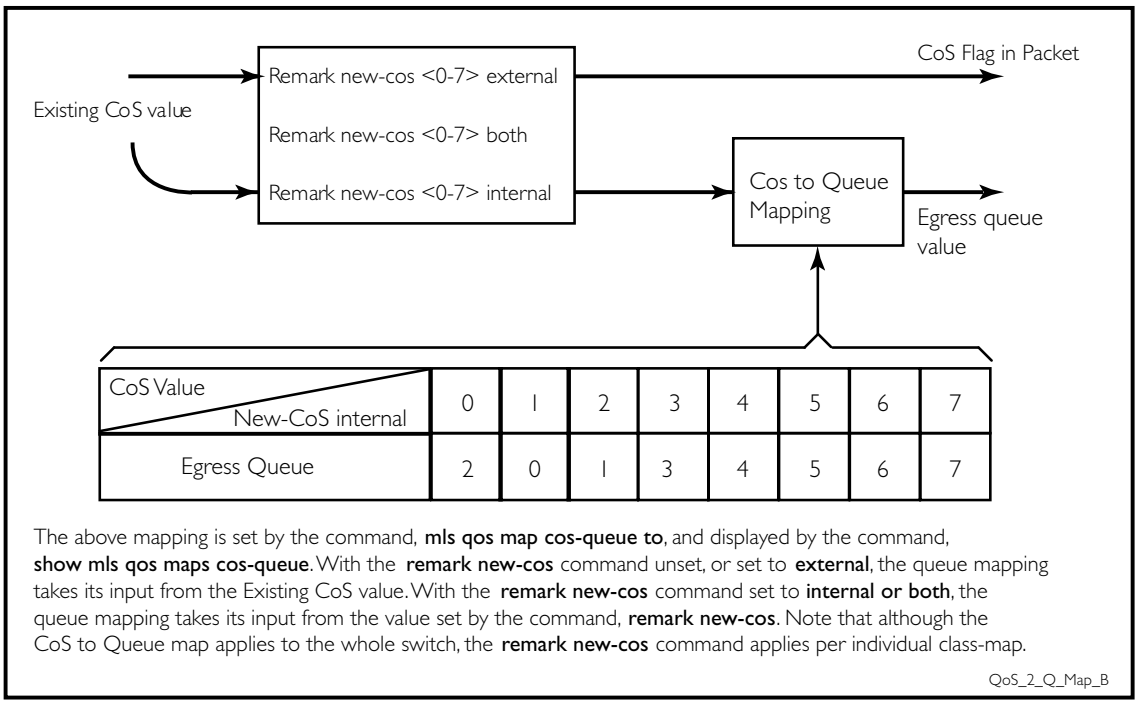


Table 28-1: CoS to egress queue remarking function

Input	Command	Output
CoS field = 1	Remark new-cos (not configured)	CoS value = 1 Packet sent to egress queue 0
CoS field = 1	Remark new-cos 2 external	CoS value = 2 Packet sent to egress queue 0
CoS set to 1	Remark new-cos 2 internal	CoS value = 1 Packet sent to egress queue 1
CoS set to 1	Remark new-cos 2 both	CoS value = 2 Packet sent to egress queue 1
Note: This table assumes that the CoS to Queue map is set to its default values.		

Example

For policy-map `pmap3` and class-map `cmap1`, set the CoS value to `2` and also set the input to the CoS to queue map so that the traffic is assigned to egress queue 1:

```
awplus# configure terminal
awplus(config)# policy-map pmap3
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# remark new-cos 2 both
```

Related Commands

mls qos map cos-queue to

show mls qos maps cos-queue

service-policy input

Overview Use this command to apply a policy-map to the input of an interface.

Use the **no** variant of this command to remove a policy-map and interface association.

Syntax

```
service-policy input <policy-map>
no service-policy input <policy-map>
```

Parameter	Description
<policy-map>	Policy map name that will be applied to the input.

Mode Interface Configuration

Usage This command can be applied to switch ports or static channel groups, but not to dynamic (LACP) channel groups.

Example To apply a policy-map named `pmap1` to interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# service-policy input pmap1
```

set ip next-hop (PBR)

Overview Use this command to configure policy-based routing. When this command is set, all packets that match a selected class-map will be forwarded to the specified next hop.

The **no** variant of this command removes the next-hop address (in the context of its policy-map and class-map) from the configuration.

Syntax

```
set ip next-hop <ip-addr>
no set ip next-hop
```

Parameter	Description
<ip-addr>	The IP address of the next hop destination.

Mode Policy Map Class Configuration

Usage In typical deployments of policy-based routing, some traffic types require conventional routing (i.e. via the routes in the IP routing table) while other traffic types require policy-based routing.

Where the traffic to be policy-routed is a subset of the traffic that is to be conventionally routed, then the configuration is reasonably simple. To configure this, make a policy-map that contains one or more class-maps that match the traffic to be policy routed. Then configure their next-hop with this command (**set ip next-hop**). The remaining traffic will be conventionally routed according to the rules set for the default class-map, providing that this is not subject to the **set ip next-hop.**

The situation becomes more complex if the traffic requiring conventional routing is a subset of the traffic to be policy-routed. To configure this, make a policy-map that contains one, or more, class-maps that match the requirement for *conventional* routing. Do not configure these class-maps with a **set ip next-hop** command. Then identify the remaining class-maps that require policy-based routing and apply the **set ip next-hop** command to them. Note that this remaining traffic could be just the default class-map, if *all* other traffic types were to be policy-routed.

Also note that the order in which the class-maps are configured in the policy-map is important, because traffic is matched against the class-maps in the order that they were assigned to the policy-map.

Example To forward packets to 192.168.1.1 if they match the class-map called cmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# set ip next-hop 192.168.1.1
```

Related commands class-map

show class-map

Overview Use this command to display the QoS class-maps' criteria for classifying traffic.

Syntax

```
show class-map [<class-map-name>]
```

Parameter	Description
<class-map-name>	Name of the class-map.

Mode User Exec and Privileged Exec

Example To display a QoS class-map's match criteria for classifying traffic, use the command:

```
awplus# show class-map cmap1
```

Output Figure 28-2: Example output from the **show class-map** command

```
CLASS-MAP-NAME: cmap1
      Set IP DSCP: 56
      Match IP DSCP: 7
```

Related Commands class-map

show mls qos

Overview Use this command to display whether QoS is enabled or disabled on the switch.

Syntax

```
show mls qos
```

Mode User Exec and Privileged Exec

Example To display whether QoS is enabled or disabled, use the command:

```
awplus# show mls qos
```

Output Figure 28-3: Example output from the **show mls qos** command

```
awplus#show mls qos
 Enable
```

Related Commands mls qos enable

show mls qos interface

Overview Displays the current settings for the interface. This includes its default CoS and queue, scheduling used for each queue, and any policies/maps that are attached.

Syntax `show mls qos interface [<port>]`

Parameter	Description
<port>	Switch port.

Mode User Exec and Privileged Exec

Example To display current CoS and queue settings for interface `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1
```

Output Figure 28-4: Example output from the **show mls qos interface** command

```
Default CoS:   7
    Default Queue: 7
    Number of egress queues: 8
    Queue Set: 1
    Egress Queue:        0
      Status:            Enabled
      Scheduler:         Strict Priority
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
    Egress Queue:        1
      Status:            Enabled
      Scheduler:         Strict Priority
      Queue Limit:       12%
      Egress Rate Limit: 0 Kb
```

```
   Egress Queue:        2
      Status:           Enabled
      Scheduler:        Strict Priority
      Queue Limit:      12%
      Egress Rate Limit: 0 Kb
    Egress Queue:       3
      Status:           Enabled
      Scheduler:        Wrr Group 2
      Weight:           10
      Queue Limit:      12%
      Egress Rate Limit: 0 Kb
    Egress Queue:       4
      Status:           Enabled
      Scheduler:        Wrr Group 1
      Weight:           10
      Queue Limit:      12%
      Egress Rate Limit: 0 Kb
```

```
    Egress Queue:       5
      Status:           Enabled
      Scheduler:        Strict Priority
      Queue Limit:      12%
      Egress Rate Limit: 0 Kb
    Egress Queue:       6
      Status:           Enabled
      Scheduler:        Strict Priority
      Queue Limit:      12%
      Egress Rate Limit: 0 Kb
    Egress Queue:       7
      Status:           Enabled
      Scheduler:        Strict Priority
      Queue Limit:      12%
      Egress Rate Limit: 0 Kb
```

Table 28-2: Parameters in the output of the **show mls qos interface** command

Parameter	Description
`Default CoS`	The default CoS priority that will be applied to all packets arriving on this interface.
`Default Queue`	The default queue that will be applied to all packets arriving on this interface.
`Number of egress queues`	The total number of egress queues available on this interface.
`Egress Queue X`	Number of this egress queue.
`Status`	Queue can either be enabled or disabled.
`Scheduler`	The scheduling mode being used for servicing the transmission of packets on this port.

Table 28-2: Parameters in the output of the **show mls qos interface** command

Parameter	Description
`Queue Limit`	The percentage of the port's buffers that have been allocated to this queue.
`Egress Rate Limit`	The amount of traffic that can be transmitted via this queue per second. 0 Kb means there is currently no rate-limiting enabled.

show mls qos interface policer-counters

Overview This command displays an interface's policer counters. This can either be for a specific class-map or for all class-maps attached to the interface. If no class-map is specified then all class-map policer counters attached to the interface are displayed.

Syntax
```
show mls qos interface <port> policer-counters [class-map
<class-map>]
```

Parameter	Description
`<port>`	Switch port.
`class-map`	Select a class-map.
`<class-map>`	Class-map name.

Mode User Exec and Privileged Exec

Usage Note that:

- The hardware does not record distinct counters for the number of Green or Yellow bytes, so the field marked Green/Yellow is the summation of bytes that have been marked Green or Yellow by the meter.
- The counters are based on metering performed on the specified class-map. Therefore, the 'Dropped Bytes' counter is the number of bytes dropped due to metering. This is different from packets dropped via a 'deny' action in the ACL. If a policer is configured to perform re-marking, bytes can be marked Red but are not dropped, and is shown with a value of 0 for the Dropped field and a non-0 value for the 'Red Bytes' field.

Example To show the counters for all class-maps attached to `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1 policer-counters
```

Output Figure 28-5: Example output from **show mls qos interface policer-counters**

```
awplus#show mls qos int port1.0.1 policer-counters
Interface:               port1.0.1
  Class-map:             default
    Green/Yellow Bytes:  0
    Red Bytes:           0
    Dropped Bytes:       0
    Non-dropped Bytes:   0
  Class-map:             cmap1
    Green/Yellow Bytes:  1629056
    Red Bytes:           7003200
    Dropped Bytes:       0
    Non-dropped Bytes:   8632256
```

This output shows a policer configured with remarking through ‘action remark-transmit’, so although bytes are marked as Red, none are dropped. Therefore, the ‘Non-dropped Bytes’ field shows a summation of Green/Yellow and Red bytes.

show mls qos interface queue-counters

Overview This command displays an interface's egress queue counters. This can either be for a specific queue or for all queues on the interface. If no queue is specified all queue counters on the interface will be displayed.

The counters show the number of frames currently in the queue and the maximum number of frames allowed in the queue, for individual egress queues and the port's queue (which will be a sum of all egress queues).

Syntax

```
show mls qos interface <port> queue-counters [queue <0-7>]
```

Parameter	Description
<port>	Switch port.
<0-7>	Queue.

Mode User Exec and Privileged Exec

Example To show the counters for all queues on `port1.0.1`, use the command:

```
awplus# show mls qos interface port1.0.1 queue-counters
```

Output Figure 28-6: Example output from the **show mls qos interface queue-counters** command

```
Interface port1.0.4 Queue Counters:
  Port queue length     1169
  Egress Queue length:
    Queue 0                0
    Queue 1                0
    Queue 2             1169
    Queue 3                0
    Queue 4                0
    Queue 5                0
    Queue 6                0
    Queue 7                0
```

Table 28-3: Parameters in the output of the **show mls qos interface queue-counters** command

Parameter	Description
`Interface`	Port we are showing the counters for.

Table 28-3: Parameters in the output of the **show mls qos interface queue-counters** command (cont.)

Parameter	Description
`Port queue length`	Number of frames in the port's queue. This will be the sum of all egress queues on the port.
`Egress Queue length`	Number of frames in a specific egress queue.

show mls qos interface storm-status

Overview Show the current configuration and status of the QoS Storm Protection (QSP) on the given port.

Syntax

```
show mls qos interface <port> storm-status
```

Parameter	Description
<port>	Switch port.

Mode User Exec and Privileged Exec

Example To see the QSP status on port1.0.1, use command:

```
awplus# show mls qos interface port1.0.1 storm-status
```

Output Figure 28-7: Example output from the **show mls qos interface storm-status** command

```
Interface:           port1.0.1
Storm-Protection:    Enabled
Port-status:         Enabled
Storm Action:        vlandisable
Storm Window:        5000 ms
Storm Downtime:      0 s
Timeout Remaining:   0 s
Last read data-rate: 0 kbps
Storm Rate:          1000 kbps
```

Related Commands

storm-action

storm-downtime

storm-protection

storm-rate

storm-window

show mls qos maps cos-queue

Overview Show the current configuration of the cos-queue map.

Syntax

```
show mls qos maps cos-queue
```

Mode User Exec and Privileged Exec

Example To display the current configuration of the cos-queue map, use the command:

```
awplus# show mls qos maps cos-queue
```

Output Figure 28-8: Example output from the **show mls qos maps cos-queue** command

```
COS-TO-QUEUE-MAP:
      COS :           0 1 2 3 4 5 6 7
      --------------------------------

    QUEUE:          0 7 1 3 4 5 6 7
```

Related Commands mls qos map cos-queue to

show mls qos maps premark-dscp

Overview This command displays the premark-dscp map. This map is used when the trust dscp command has been specified for a policy-map's class-map to replace the DSCP, CoS and/or bandwidth class of a packet matching the class-map based on a lookup DSCP value.

Syntax

```
show mls qos maps premark-dscp [<0-63>]
```

Parameter	Description
<0-63>	DSCP table entry.

Mode User Exec and Privileged Exec

Example To display the premark-dscp map for DSCP 1, use the command:

```
awplus# show mls qos maps premark-dscp 1
```

Output Figure 28-9: Example output from the **show mls qos maps premark-dscp** command

```
PREMARK-DSCP-MAP:

    DSCP 1
    Bandwidth Class
    -------------------------
    New DSCP               2
    New CoS                0
    New Bandwidth Class    green
```

Related Commands mls qos map premark-dscp to

trust dscp

show platform classifier statistics utilization brief

Overview This command displays the number of used entries available for various platform functions, and the percentage that number of entries represents of the total available.

Syntax

```
show platform classifier statistics utilization brief
```

Mode Privileged Exec

Example To display the platform classifier utilization statistics, use the following command:

```
awplus# show platform classifier statistics utilization brief
```

Output Figure 28-10: Output from the **show platform classifier statistics utilization brief** command

```
awplus#show platform classifier statistics utilization brief

[Instance 0]
  Number of Entries:
  Policy Type      Group ID   Used / Total
  ---------------------------------------------
  ACL              1476395009    0 /  118 (  0%)
  Web Auth         Inactive      0 /    0 (  0%)
  QoS                            0 /  128 (  0%)
```

Related Commands show platform

show policy-map

Overview Displays the policy-maps configured on the switch. The output also shows whether or not they are connected to a port (attached / detached) and shows their associated class-maps.

Syntax

```
show policy-map [<name>]
```

Parameter	Description
<name>	The name of a specific policy-map.

Mode User Exec and Privileged Exec

Example To display a listing of the policy-maps configured on the switch, use the command:

```
awplus# show policy-map
```

Output Figure 28-11: Example output from the **show policy-map** command

```
POLICY-MAP-NAME: general-traffic
  State: attached
    Default class-map action: permit
    CLASS-MAP-NAME: default
    CLASS-MAP-NAME: database-traffic
```

Related Commands service-policy input

storm-action

Overview Sets the action to be taken when triggered by QoS Storm Protection (QSP). There are three available options:

- **portdisable** will disable the port in software.
- **vlandisable** will disable the port from the VLAN matched by the class-map in class-map.
- **linkdown** will physically bring the port down. The **vlandisable** requires the match vlan class-map to be present in the class-map.

The **no** variant of this command will negate the action set by the **storm-action** command.

Syntax

```
storm-action {portdisable|vlandisable|linkdown}
no storm-action
```

Parameter	Description
`portdisable`	Disable the port in software.
`vlandisable`	Disable the VLAN.
`linkdown`	Shutdown the port physically.

Mode Policy Map Class Configuration

Examples To apply the storm protection of `vlandisable` to the policy-map named `pmap2`, and the class-map named `cmap1`, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c# storm-action vlandisable
```

To negate the storm protection set on the policy-map named `pmap2`, and the class-map named `cmap1`, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c# no storm-action
```

Related Commands

storm-downtime

storm-protection

storm-rate

storm-window

storm-downtime

Overview Sets the time to re-enable a port that has been disabled by QoS Storm Protection (QSP). The time is given in seconds, from a minimum of one second to maximum of 86400 seconds (i.e. one day).

The **no** variant of this command resets the time to the default value of 10 seconds.

Syntax

```
storm-downtime <1-86400>
no storm-downtime
```

Parameter	Description
<1-86400>	Seconds.

Default 10 seconds

Mode Policy Map Class Configuration

Examples To re-enable the port in 1 minute, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# storm-downtime 60
```

To re-set the port to the default (10 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap1
awplus(config-pmap-c)# no storm-downtime
```

Related Commands

storm-action

storm-protection

storm-rate

storm-window

storm-protection

Overview Use this command to enable Policy Based Storm Protection (such as QSP - QoS Storm Protection). Storm protection is activated as soon as a port is enabled. However, it will only be functional after storm-rate and storm-window have been set.

The **no** variant of this command disables Policy Based Storm Protection.

Syntax

```
storm-protection
no storm-protection
```

Default By default, storm protection is disabled.

Mode Policy Map Class Configuration

Examples To enable QSP on cmap2 in pmap2, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-protection
```

To disable QSP on cmap2 in pmap2, use the following commands:

```
awplus# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-protection
```

Related Commands

storm-action

storm-downtime

storm-rate

storm-window

storm-rate

Overview Sets the data rate that triggers the storm-action. The rate is in kbps and the range is from 1kbps to 40Gbps.

Note that this setting is made in conjunction with the storm-window command.

Use the **no** variant of this command to negate the **storm-rate** command.

Syntax

```
storm-rate <1-40000000>
no storm-rate
```

Parameter	Description
<1-40000000>	The range of the storm-rate.

Default No default

Mode Policy Map Class Configuration

Usage This setting is made in conjunction with the storm-window command.

Examples To limit the data rate to 100Mbps, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-rate 100000
```

To negate the limit set previously, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-rate
```

Related Commands

storm-action

storm-downtime

storm-protection

storm-window

storm-window

Overview Sets the window size of QoS Storm Protection (QSP). This sets the time to poll the data-rate every given milliseconds. Minimum window size is 100 ms and the maximum size is 60 sec.

Use the **no** variant of this command to negate the **storm-window** command.

Syntax

```
storm-window <100-60000>
no storm-window
```

Parameter	Description
<100-60000>	The window size, measured in milliseconds.

Default No default

Mode Policy Map Class Configuration

Usage This command should be set in conjunction with the storm-rate command.

Examples To set the QSP window size to `5000` ms, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# storm-window 5000
```

To negate the QSP window size set previously, use the following commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap2
awplus(config-pmap)# class cmap2
awplus(config-pmap-c)# no storm-window
```

Related Commands

storm-action

storm-downtime

storm-protection

storm-rate

trust dscp

Overview This command enables the premark-dscp map to replace the bandwidth-class, CoS, DSCP, and queue of classified traffic based on a lookup DSCP value.

With the **no** variant of this command, no premark-dscp mapping function will be applied for the selected class-map.QoS components of the packet existing either at ingress, or applied by the class-map, will pass unchanged.

Syntax

```
trust dscp
no trust
```

Mode Policy-Map Configuration. Because policy-maps are applied to ports, you can think of **trust dscp** as a per-port setting.

Examples To enable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# trust dscp
```

To disable the premark-dscp map lookup for policy-map pmap1, use the commands:

```
awplus# configure terminal
awplus(config)# policy-map pmap1
awplus(config-pmap)# no trust
```

Related Commands mls qos map premark-dscp to

wrr-queue disable queues

Overview Use this command to disable an egress queue from transmitting traffic.

The **no** variant of this command enables an egress queue to transmit traffic.

Syntax

```
wrr-queue disable queues [0][1][2][3][4][5][6][7]
no wrr-queue disable queues [0][1][2][3][4][5][6][7]
```

Parameter	Description
`[0][2]...[7]`	Selects one or more queues numbered 0 to 7.

Mode Interface Configuration

Examples To disable queue 1 from transmitting traffic, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue disable queues 1
```

To enable queue 1 to transmit traffic, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no wrr-queue disable queues 1
```

Related Commands show mls qos interface

wrr-queue egress-rate-limit queues

Overview Sets a limit on the amount of traffic that can be transmitted per second from these queues. The default unit is in Kb, but Mb or Gb can also be specified. The minimum is 651Kb.

Syntax

```
wrr-queue egress-rate-limit <bandwidth> queues
{0}[1][2][3][4][5][6][7]
```

```
no wrr-queue egress-rate-limit <bandwidth> queues
{0}[1][2][3][4][5][6][7]
```

Parameter	Description
<bandwidth>	Bandwidth <1-40000000 kbits> (usable units: k, m, g).
{0}[1]...[7]	Selects one or more queues to apply the bandwidth limit to as specified in the preceding *<bandwidth>* parameter.

Mode Interface Configuration

Example To limit the egress rate of queues 0, 1 and 2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue egress-rate-limit 500M queues 0 1
2
```

Related Commands show mls qos interface

wrr-queue weight queues

Overview This command configures weighted round-robin based scheduling on the specified egress queues on switch port interfaces only. The weights are specified as ratios relative to each other.

Syntax

```
wrr-queue weight <1-15> queues [0][1][2][3][4][5][6][7]
```

Parameter	Description
<1-15>	Weight (the higher the number the greater will be the queue servicing).
`[0][1]...[7]`	Enter egress queue numbers 0-7, to assign the specified queues the specified weight.

Mode Interface Configuration for switch port interfaces only (not for static aggregated interfaces).

Usage Only apply weighted round-robin based scheduling to switch port interfaces (for example, `awplus(config)#interface port1.0.2`).

You cannot apply weighted round-robin based scheduling to static aggregated interfaces (for example, `awplus(config)#interface sa2`). Attempting to apply weighted round-robin based scheduling on aggregated interfaces will display the console error shown below:

```
awplus# configure terminal
awplus(config)# interface sa2
awplus(config-if)# wrr-queue weight
% Invalid input detected at ^ marker
```

Example To apply a WRR weight of `6` to queues 0 and 1 on port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# wrr-queue weight 6 queues 0 1
```

Related Commands priority-queue

show mls qos interface

29 802.1X Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure 802.1X port access control.

Command List

dot1x accounting

Overview This command overrides the **default** RADIUS accounting method for IEEE 802.1X-based authentication on an interface by allowing you to apply a user-defined named method list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method list.

Syntax

```
dot1x accounting {default|<list-name>}
no dot1x accounting
```

Parameter	Description
default	Apply the default accounting method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Mode

Example To apply the named list 'vlan10_acct' on the `vlan10` interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# dot1x accounting vlan10_acct
```

To remove the named list from the `vlan10` interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no dot1x accounting
```

Related Commands aaa accounting dot1x

dot1x authentication

Overview This command overrides the **default** 802.1X-based authentication method on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
dot1x authentication {default|<list-name>}
no dot1x authentication
```

Parameter	Description
default	Apply the default authentication method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Mode

Example To apply the named list 'vlan10_auth' on the `vlan10` interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# dot1x authentication vlan10_auth
```

To remove the named list from the `vlan10` interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no dot1x authentication
```

Related Commands aaa authentication dot1x

debug dot1x

Overview Use this command to enable 802.1X IEEE Port-Based Network Access Control troubleshooting functions.

Use the **no** variant of this command to disable this function.

Syntax

```
debug dot1x [all|auth-web|event|nsm|packet|timer]
no debug all dot1x
no debug dot1x [all|auth-web|event|nsm|packet|timer]
```

Parameter	Description
`all`	Used with the **no** variant of this command exclusively; turns off all debugging for 802.1X.
`auth-web`	Specifies debugging for 802.1X auth-web information.
`events`	Specifies debugging for 802.1X events.
`nsm`	Specifies debugging for NSM messages.
`packet`	Specifies debugging for 802.1X packets.
`timer`	Specifies debugging for 802.1X timers.

Mode Privileged Exec and Global Configuration

Usage This command turns on a mode where trace-level information is output during? authentication conversations. Be aware that this is a very verbose output.? It is mostly useful to capture this as part of escalating an issue to ATI support.

Examples Use this command without any parameters to turn on normal 802.1X debug information.

```
awplus# debug dot1x
awplus# show debugging dot1x
```

```
802.1X debugging status:
  802.1X events debugging is
  802.1X timer debugging is on
  802.1X packets debugging is on
  802.1X NSM debugging is on
```

Related Commands show debugging dot1x

undebug dot1x

dot1x control-direction

Overview This command sets the direction of the filter for the unauthorized interface.

If the optional **in** parameter is specified with this command then packets entering the specified port are discarded. The **in** parameter discards the ingress packets received from the supplicant.

If the optional **both** parameter is specified with this command then packets entering (ingress) and leaving (egress) the specified port are discarded. The **both** parameter discards the packets received from the supplicant and sent to the supplicant.

The **no** variant of this command sets the direction of the filter to **both**. The port will then discard both ingress and egress traffic.

Syntax

```
dot1x control-direction {in|both}
no dot1x control-direction
```

Parameter	Description
`in`	Discard received packets from the supplicant (ingress packets).
`both`	Discard received packets from the supplicant (ingress packets) and transmitted packets to the supplicant (egress packets).

Default The authentication port direction is set to **both** by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the port direction to the default (**both**) for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x control-direction
```

To set the port direction to **in** for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x control-direction in
```

To set the port direction to **in** for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x control-direction in
```

To set the port direction to the default (**both**) for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no dot1x control-direction
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show auth interface

dot1x eap

Overview This command selects the transmit mode for the EAP packet. If the authentication feature is not enabled then EAP transmit mode is not enabled. The default setting discards EAP packets.

Syntax

```
dot1x eap {discard|forward|forward-untagged-vlan|forward-vlan}
```

Parameter	Description
`discard`	Discard.
`forward`	Forward to all ports on the switch.
`forward-untagged-vlan`	Forward to ports with the same untagged VLAN.
`forward-vlan`	Forward to ports with the same VLAN.

Default The transmit mode is set to `discard` EAP packets by default.

Mode Global Configuration

Examples To set the transmit mode of EAP packet to `forward` to forward EAP packets to all ports on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward
```

To set the transmit mode of EAP packet to `discard` to discard EAP packets, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap discard
```

To set the transmit mode of EAP packet to `forward-untagged-vlan` to forward EAP packets to ports with the same untagged vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-untagged-vlan
```

To set the transmit mode of EAP packet to `forward-vlan` to forward EAP packets to ports with the same vlan, use the commands:

```
awplus# configure terminal
awplus(config)# dot1x eap forward-vlan
```

dot1x eapol-version

Overview This command sets the EAPOL protocol version for EAP packets when 802.1X port authentication is applied.

Use the **no** variant of this command to set the EAPOL protocol version to 1.

The default EAPOL protocol version is version 1.

Syntax

```
dot1x eapol-version {1|2}
no dot1x eapol-version
```

Parameter	Description
1	EAPOL version.
2	EAPOL version.

Default The EAP version for 802.1X authentication is set to 1 by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the EAPOL protocol version to `2` for `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x eapol-version
```

To set the EAPOL protocol version to 2 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x eapol-version 2
```

To set the EAPOL protocol version to the default version (1) for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no dot1x eapol-version
```

Validation Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

dot1x initialize interface

Overview This command removes authorization for a connected **interface** with the specified<*interface-list*>. The connection will attempt to re-authorize when the specified **port** attempts to make use of the network connection.

NOTE: *Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the interface trying to access the network resources.*

Syntax

```
dot1x initialize interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.6`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.2-1.0.4`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Examples To initialize 802.1X port authentication on the interface `port1.0.2`, use the command:

```
awplus# dot1x initialize interface port1.0.2
```

To unauthorize switch `port1.0.1` and attempt reauthentication on switch `port1.0.1`, use the command:

```
awplus# dot1x initialize interface port1.0.1
```

To unauthorize all switch ports for a 24-port device and attempt reauthentication, use the command:

```
awplus# dot1x initialize interface port1.0.1-port1.0.24
```

Validation Commands show dot1x

show dot1x interface

Related Commands dot1x initialize supplicant

dot1x initialize supplicant

Overview This command removes authorization for a connected `supplicant` with the specified **MAC address** or **username**. The connection will attempt to re-authorize when the specified supplicant attempts to make use of the network connection.

NOTE: *Reauthentication could be a long time after the use of this command because the reauthorization attempt is not triggered by this command. The attempt is triggered by the first packet from the supplicant trying to access the network resources.*

Syntax

```
dot1x initialize supplicant {<macadd>|username}
```

Parameter	Description
`dot1x`	IEEE 802.1X Port-Based Access Control.
`initialize`	Initialize the port to attempt reauthentication.
`supplicant`	Specify the supplicant to initialize.
<macadd>	MAC (hardware address of the supplicant.
`username`	The name of the supplicant entry.

Mode Privileged Exec

Example To initialize the supplicant authentication, use the commands

```
awplus# configure terminal
awplus(config)# dot1x initialize supplicant 0090.99ab.a020
awplus(config)# dot1x initialize supplicant guest
```

Validation Commands show dot1x

show dot1x supplicant

Related Commands dot1x initialize interface

dot1x keytransmit

Overview This command enables key transmission on the interface specified previously in Interface mode.

The **no** variant of this command disables key transmission on the interface specified.

Syntax

```
dot1x keytransmit
no dot1x keytransmit
```

Default Key transmission for port authentication is enabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage Use this command to enable key transmission over an Extensible Authentication Protocol (EAP) packet between the authenticator and supplicant. Use the **no** variant of this command to disable key transmission.

Examples To enable the key transmit feature on interface `port1.0.2`, after it has been disabled by negation, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x keytransmit
```

To disable the key transmit feature from the default startup configuration on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x keytransmit
```

Validation Commands show dot1x

show dot1x interface

dot1x max-auth-fail

Overview Use this command to configure the maximum number of login attempts for a supplicant (client device) using the **auth-fail vlan** feature, when using 802.1X port authentication on an interface.

The **no** variant of this command resets the maximum login attempts for a supplicant (client device) using the auth-fail vlan feature, to the default configuration of 3 login attempts.

Syntax

```
dot1x max-auth-fail <0-10>
no dot1x max-auth-fail
```

Parameter	Description
<0-10>	Specify the maximum number of login attempts for supplicants on an interface using 802.1X port authentication.

Default The default maximum number of login attempts for a supplicant on an interface using 802.1X port authentication is three (3) login attempts.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage This command sets the maximum number of login attempts for supplicants on an interface. The supplicant is moved to the auth-fail VLAN from the Guest VLAN after the number of failed login attempts using 802.1X authentication is equal to the number set with this command.

See the Authentication Feature Overview and Configuration Guide for information about:

- the auth-fail VLAN feature, and
- restrictions regarding combinations of authentication enhancements working together

Examples To configure the maximum number of login attempts for a supplicant on interface `port1.0.2` to a single (1) login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-auth-fail 1
```

To configure the maximum number of login attempts for a supplicant on interface `port1.0.2` to the default number of three (3) login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-auth-fail
```

To configure the maximum number of login attempts for a supplicant on authentication profile 'student' to a single (1) login attempt, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x max-auth-fail 1
```

To configure the maximum number of login attempts for a supplicant on authentication profile 'student' to the default number of three (3) login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no dot1x max-auth-fail
```

Validation Commands

show running-config

show dot1x interface

Related Commands

auth auth-fail vlan

auth profile (Global Configuration)

dot1x max-reauth-req

dot1x max-reauth-req

Overview This command sets the number of reauthentication attempts before an interface is unauthorized.

The **no** variant of this command resets the reauthentication delay to the default.

Syntax

```
dot1x max-reauth-req <1-10>
no dot1x max-reauth-req
```

Parameter	Description
<1-10>	Specify the maximum number of reauthentication attempts for supplicants on an interface using 802.1X port authentication.

Default The default maximum reauthentication attempts for interfaces using 802.1X port authentication is two (2) reauthentication attempts, before an interface is unauthorized.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Use this command to set the maximum reauthentication attempts after failure.

Examples To configure the maximum number of reauthentication attempts for interface `port1.0.2` to a single (1) reauthentication request, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x max-reauth-req 1
```

To configure the maximum number of reauthentication attempts for interface `port1.0.2` to the default maximum number of two (2) reauthentication attempts, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x max-reauth-req
```

To configure the maximum number of reauthentication attempts for authentication profile 'student' to a single (1) reauthentication request, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x max-reauth-req 1
```

To configure the maximum number of reauthentication attempts for authentication profile 'student' to the default maximum number of two (2) reauthentication attempts, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no dot1x max-reauth-req
```

Validation Commands

show running-config

Related Commands

auth profile (Global Configuration)

dot1x max-auth-fail

show dot1x interface

dot1x port-control

Overview This command enables 802.1X port authentication on the interface specified, and sets the control of the authentication port.

The **no** variant of this command disables the port authentication on the interface specified.

Syntax

```
dot1x port-control {force-unauthorized|force-authorized|auto}
no dot1x port-control
```

Parameter	Description
`force-unauthorized`	Force the port state to unauthorized. Specify this to force a port to always be in an unauthorized state.
`force-authorized`	Force the port state to authorized. Specify this to force a port to always be in an authorized state.
`auto`	Allow the port client to negotiate authentication. Specify this to enable authentication on the port.

Default 802.1X port control is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Use this command to force a port state.

When **port-control** is set to **auto**, the 802.1X authentication feature is executed on the interface, but only if the **aaa authentication dot1x** command has been issued.

Examples To enable port authentication on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
```

To enable port authentication force authorized on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control force-authorized
```

To disable port authentication on the interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x port-control
```

To enable port authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x port-control auto
```

To enable port authentication force authorized on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x port-control
force-authorized
```

To disable port authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no dot1x port-control
```

Validation Commands show dot1x interface

Related Commands aaa authentication dot1x

auth profile (Global Configuration)

dot1x timeout tx-period

Overview This command sets the transmit timeout for the authentication request on the specified interface.

The **no** variant of this command resets the transmit timeout period to the default (30 seconds).

Syntax

```
dot1x timeout tx-period <1-65535>
no dot1x timeout tx-period
```

Parameter	Description
<1-65535>	Seconds.

Default The default transmit period for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Use this command to set the interval between successive attempts to request an ID.

Examples To set the transmit timeout period to 5 seconds on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x timeout tx-period 5
```

To reset transmit timeout period to the default (30 seconds) on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no dot1x timeout tx-period
```

To set the transmit timeout period to 5 seconds on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# dot1x timeout tx-period 5
```

To reset transmit timeout period to the default (30 seconds) on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no dot1x timeout tx-period
```

Validation Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show debugging dot1x

Overview Use this command to display the 802.1X debugging option set.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show debugging dot1x
```

Mode User Exec and Privileged Exec

Usage This is a sample output from the `show debugging dot1x` command.

```
awplus# debug dot1x
awplus# show debugging dot1x
```

```
802.1X debugging status:
  802.1X events debugging is on
  802.1X timer debugging is on
  802.1X packets debugging is on
  802.1X NSM debugging is on
```

Related Commands debug dot1x

show dot1x

Overview This command shows authentication information for dot1x (802.1X) port authentication.

If you specify the optional **all** parameter then this command also displays all authentication information for each port available on the switch.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show dot1x [all]
```

Parameter	Description
`all`	Displays all authentication information for each port available on the switch.

Mode Privileged Exec

Example

```
awplus# show dot1x all
```

Table 1: Example output from the **show dot1x** command

```
awplus# show dot1x all
802.1X Port-Based Authentication Enabled
RADIUS server address: 150.87.18.89:1812
Next radius message id: 5
RADIUS client address: not configured
Authentication info for interface port1.0.6
portEnabled: true - portControl: Auto
portStatus: Authorized
reAuthenticate: disabled
reAuthPeriod: 3600
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
PAE: connectTimeout: 30
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in
KT: keyTxEnabled: false
critical: disabled
guestVlan: disabled
dynamicVlanCreation: single-dynamic-vlan
assignFailActionRule: deny
hostMode: multi-supplicant
maxSupplicant: 1024
```

Table 1: Example output from the **show dot1x** command (cont.)

```
dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
twoStepAuthentication:
    configured: enabled
    actual: enabled
SupplicantMac: none
supplicantMac: none
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
   authenticationMethod: 802.1X Authentication
   portStatus: Authorized - currentId: 1
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
   BE: state: Idle - reqCount: 0 - idFromServer: 0
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
   criticalState: off
   dynamicVlanId: 2
802.1X statistics for interface port1.0.6
   EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
   EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
   EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame Src:  00d0.59ab.7037
Authentication session statistics for interface port1.0.6
   session user name: manager
   session authentication method: Remote server
   session time: 19440 secs
   session terminate cause: Not terminated yet
Authentication Diagnostics for interface port1.0.6
   Supplicant address: 00d0.59ab.7037
   authEnterConnecting: 2
   authEaplogoffWhileConnecting: 1
   authEnterAuthenticating: 2
   authSuccessWhileAuthenticating: 1
   authTimeoutWhileAuthenticating: 1
   authFailWhileAuthenticating: 0
   authEapstartWhileAuthenticating: 0
```

Table 1: Example output from the **show dot1x** command (cont.)

```
    authEaplogoggWhileAuthenticating: 0
    authReauthsWhileAuthenticated: 0
    authEapstartWhileAuthenticated: 0
    authEaplogoffWhileAuthenticated: 0
    BackendResponses: 2
    BackendAccessChallenges: 1
    BackendOtherrequestToSupplicant: 3
    BackendAuthSuccess: 1
    BackendAuthFails: 0
```

show dot1x diagnostics

Overview This command shows 802.1X authentication diagnostics for the specified interface (optional), which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show dot1x diagnostics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify a port to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.2-1.0.4`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example See the sample output below showing 802.1X authentication diagnostics for `port1.0.5`:

```
awplus# show dot1x diagnostics interface port1.0.5
```

Output Figure 29-1: Example output from the **show dot1x diagnostics** command

```
Authentication Diagnostics for interface port1.0.5
   Supplicant address: 00d0.59ab.7037
      authEnterConnecting: 2
      authEaplogoffWhileConnecting: 1
      authEnterAuthenticating: 2
      authSuccessWhileAuthenticating: 1
      authTimeoutWhileAuthenticating: 1
      authFailWhileAuthenticating: 0
      authEapstartWhileAuthenticating: 0
      authEaplogoggWhileAuthenticating: 0
      authReauthsWhileAuthenticated: 0
      authEapstartWhileAuthenticated: 0
      authEaplogoffWhileAuthenticated: 0
      BackendResponses: 2
      BackendAccessChallenges: 1
      BackendOtherrequestToSupplicant: 3
      BackendAuthSuccess: 1
```

show dot1x interface

Overview This command shows the status of 802.1X port-based authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interfaces. Use the optional **statistics** parameter to show authentication diagnostics for the specified interfaces. Use the optional **supplicant** parameter to show the supplicant state for the specified interfaces.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show dot1x interface <interface-list>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.3-1.0.5`. Do not mix interface types in a list The specified interfaces must exist.
`diagnostics`	Diagnostics.
`sessionstatistics`	Session Statistics.
`statistics`	Statistics.
`supplicant`	Supplicant.
`brief`	Brief summary of supplicant state.

Mode Privileged Exec

Examples See the sample output below showing 802.1X authentication status for `port1.0.6`:

```
awplus# show dot1x interface port1.0.6
```

Table 2: Example output from the **show dot1x interface** command for a port

```
awplus#show dot1x interface port1.0.6Authentication info for
interface port1.0.6
   portEnabled: true - portControl: Auto
   portStatus: Authorized
   reAuthenticate: disabled
   reAuthPeriod: 3600
   PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
   PAE: connectTimeout: 30
   BE: suppTimeout: 30 - serverTimeout: 30
   CD: adminControlledDirections: in
   KT: keyTxEnabled: false
   critical: disabled
   guestVlan: disabled
   dynamicVlanCreation: single-dynamic-vlan
       assignFailActionRule: deny
   hostMode: multi-supplicant
       maxSupplicant:1024
dot1x: enabled
protocolVersion: 1
authMac: enabled
method: PAP
reauthRelearning: disabled
authWeb: enabled
method: PAP
lockCount: 3
packetForwarding: disabled
    twoStepAuthentication:
       configured: enabled
       actual: enabled
supplicantMac: none
```

See the sample output below showing 802.1X authentication `sessionstatistics` for `port1.0.6`:

```
awplus# show dot1x interface port1.0.6 sessionstatistics
```

```
awplus#show dot1x interface port1.0.6
sessionstatistics
Authentication session statistics for interface
port1.0.6
   session user name: manager
       session authentication method: Remote server
       session time: 19440 secs
       session terminat cause: Not terminated yet
```

See sample output below showing 802.1X authentication `diagnostics` for `port1.0.6`:

```
awplus# show dot1x interface port1.0.6 diagnostics
```

```
awplus#show dot1x interface port1.0.6 diagnostics
Authentication Diagnostics for interface port1.0.6
   Supplicant address: 00d0.59ab.7037
      authEnterConnecting: 2
      authEaplogoffWhileConnecting: 1
      authEnterAuthenticating: 2
      authSuccessWhileAuthenticating: 1
      authTimeoutWhileAuthenticating: 1
      authFailWhileAuthenticating: 0
      authEapstartWhileAuthenticating: 0
      authEaplogoggWhileAuthenticating: 0
      authReauthsWhileAuthenticated: 0
      authEapstartWhileAuthenticated: 0
      authEaplogoffWhileAuthenticated: 0
      BackendResponses: 2
      BackendAccessChallenges: 1
      BackendOtherrequestToSupplicant: 3
      BackendAuthSuccess: 1
```

See sample output below showing the `supplicant` on the interface `port1.0.6`:

```
awplus# show dot1x interface port1.0.6 supplicant
```

```
awplus#show dot1x interface port1.0.6 supplicant
authenticationMethod: dot1x
   totalSupplicantNum: 1
   authorizedSupplicantNum: 1
      macBasedAuthenticationSupplicantNum: 0
      dot1xAuthenticationSupplicantNum: 1
      webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
      authenticationMethod: dot1x
      portStatus: Authorized - currentId: 4
      abort:F fail:F start:F timeout:F success:T
      PAE: state: Authenticated - portMode: Auto
      PAE: reAuthCount: 0 - rxRespId: 0
      PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
      BE: state: Idle - reqCount: 0 - idFromServer: 3
      BE: suppTimeout: 30 - serverTimeout: 30
      CD: adminControlledDirections: in -
operControlledDirections: in
      CD: bridgeDetected: false
      KR: rxKey: false
      KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing 802.1X (`dot1x`) authentication statistics for `port1.0.6`:

```
awplus# show dot1x statistics interface port1.0.6
```

```
awplus#show dot1x statistics interface port1.0.6802.1X statistics
for interface port1.0.6
    EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
    EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
    EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
    EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
    Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
    EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

Table 29-1: Parameters in the output of **show dot1x interface**

Parameter	Description
portEnabled	Interface operational status (Up-true/down-false).
portControl	Current control status of the port for 802.1X control.
portStatus	802.1X status of the port (authorized/unauthorized).
reAuthenticate	Reauthentication enabled/disabled status on port.
reAuthPeriod	Value holds meaning only if reauthentication is enabled.
abort	Indicates that authentication should be aborted when set to true.
fail	Indicates failed authentication attempt when set to false.
start	Indicates authentication should be started when set to true.
timeout	Indicates authentication attempt timed out when set to true.
success	Indicates authentication successful when set to true.
state	Current 802.1X operational state of interface.
mode	Configured 802.1X mode.
reAuthCount	Reauthentication count.
quietperiod	Time between reauthentication attempts.
reAuthMax	Maximum reauthentication attempts.
BE	Backend authentication state machine variables and constants.
state	State of the state machine.
reqCount	Count of requests sent to server.

Table 29-1: Parameters in the output of **show dot1x interface** (cont.)

Parameter	Description
suppTimeout	Supplicant timeout.
serverTimeout	Server timeout.
maxReq	Maximum requests to be sent.
CD	Controlled Directions State machine.
adminControlledDir ections	Administrative value (Both/In).
operControlledDire ctions	Operational Value (Both/In).
KR	Key receive state machine.
rxKey	True when EAPOL-Key message is received by supplicant or authenticator. false when key is transmitted.
KT	Ket Transmit State machine.
keyAvailable	False when key has been transmitted by authenticator, true when new key is available for key exchange.
keyTxEnabled	Key transmission enabled/disabled status.

Related Commands

show auth diagnostics

show dot1x sessionstatistics

show dot1x statistics interface

show dot1x supplicant interface

show dot1x sessionstatistics

Overview This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax `show dot1x sessionstatistics [interface <interface-list>]`

Parameter	Description
`interface`	Specify a port to show.
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example See sample output below showing 802.1X (`dot1x`) authentication session statistics for `port1.0.6`:

```
awplus# show dot1x sessionstatistics interface port1.0.6
```

```
Authentication session statistics for interface
port1.0.6
   session user name: manager
      session authentication method: Remote server
      session time: 19440 secs
      session terminat cause: Not terminated yet
```

show dot1x statistics interface

Overview This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax `show dot1x statistics interface <interface-list>`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example See sample output below showing 802.1X authentication statistics for `port1.0.6`:

```
awplus# show dot1x statistics interface port1.0.6
```

```
802.1X statistics for interface port1.0.6
   EAPOL Frames Rx: 5 - EAPOL Frames Tx: 16
   EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0
   EAP Rsp/Id Frames Rx: 3 - EAP Response Frames Rx: 2
   EAP Req/Id Frames Tx: 8 - EAP Request Frames Tx: 2
   Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0
   EAPOL Last Frame Version Rx: 1 - EAPOL Last Frame
Src:00d0.59ab.7037
```

show dot1x supplicant

Overview This command shows the supplicant state of the authentication mode set for the switch.

This command shows a summary when the optional **brief** parameter is used.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show dot1x supplicant [<macadd>] [brief]
```

Parameter	Description
<macadd>	MAC (hardware) address of the Supplicant.
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Example See sample output below showing the 802.1X authenticated supplicant on the switch:

```
awplus# show dot1x supplicant
```

```
authenticationMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0
Supplicant name: manager
Supplicant address: 00d0.59ab.7037
   authenticationMethod: dot1x
    Two-Step Authentication:
      firstAuthentication: Pass - Method: mac
      secondAuthentication: Pass - Method: dot1x
portStatus: Authorized - currentId: 4
abort:F fail:F start:F timeout:F success:T
PAE: state: Authenticated - portMode: Auto
PAE: reAuthCount: 0 - rxRespId: 0
PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
BE: state: Idle - reqCount: 0 - idFromServer: 3
BE: suppTimeout: 30 - serverTimeout: 30
CD: adminControlledDirections: in - operControlledDirections: in
CD: bridgeDetected: false
KR: rxKey: false
KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant 00d0.59ab.7037 brief
```

```
Interface port1.0.6
   authenticationMethod: dot1x
   totalSupplicantNum: 1
   authorizedSupplicantNum: 1
      macBasedAuthenticationSupplicantNum: 0
      dot1xAuthenticationSupplicantNum: 1
      webBasedAuthenticationSupplicantNum: 0
Interface   VID Mode MAC Address      Status         IP Address      Username
=========   === ==== ===========      ======         ==========      ========
port1.0.6
  2    D    00d0.59ab.7037   Authenticated  192.168.2.201   manager
```

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant brief
```

For example, if two-step authentication is configured with 802.1X authentication as the first method and web authentication as the second method then the output is as follows:

```
Interface port1.0.6  authenticationMethod: dot1x/web
  Two-Step Authentication
    firstMethod: dot1x
    secondMethod: web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= =============== ========
port1.0.6
  5    W    0008.0d5e.c216 Authenticated     192.168.1.200   web
```

Related Commands show dot1x supplicant interface

show dot1x supplicant interface

Overview This command shows the supplicant state of the authentication mode set for the interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

This command shows a summary when the optional **brief** parameter is used.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax `show dot1x supplicant interface <interface-list> [brief]`

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`brief`	Brief summary of the Supplicant state.

Mode Privileged Exec

Examples See sample output below showing the supplicant on the interface `port1.0.6`:

```
awplus# show dot1x interface port1.0.6
```

```
Interface port1.0.6 authenticationMethod: dot1x
  totalSupplicantNum: 1
 authorizedSupplicantNum: 1
   macBasedAuthenticationSupplicantNum: 0
   dot1xAuthenticationSupplicantNum: 1
   webBasedAuthenticationSupplicantNum: 0
   otherAuthenticationSupplicantNum: 0

 Supplicant name: VCSPCVLAN10
 Supplicant address: 0000.cd07.7b60
   authenticationMethod: 802.1X
 Two-Step Authentication:
   firstAuthentication: Pass - Method: mac
   secondAuthentication: Pass - Method: dot1x
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections:in -
operControlledDirections:in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

See sample output below showing the supplicant on the switch using the `brief` parameter:

```
awplus# show dot1x supplicant interface brief
```

```
Interface port1.0.6
   authenticationMethod: dot1x
Two-Step Authentication:
   firstMethod: mac
   secondMethod: dot1x
totalSupplicantNum: 1
authorizedSupplicantNum: 1
macBasedAuthenticationSupplicantNum: 0
dot1xAuthenticationSupplicantNum: 1
webBasedAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address     Status          IP Address      Username
=========   ===  ==== ===========     ======          ==========      ========
port1.0.6
  2    D    00d0.59ab.7037  Authenticated   192.168.2.201   manager
```

See the sample output below for static channel group (static aggregator) interface `sa1`:

```
awplus# show dot1x interface sa1 supplicant brief
```

```
awplus#show dot1x interface sa1 supplicant brief
Interface sa1
  authenticationMethod: dot1x
Two-Step Authentication:
   firstMethod: mac
   secondMethod: dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
     dot1xAuthenticationSupplicantNum: 1
     webBasedAuthenticationSupplicantNum: 0
     otherAuthenticationSupplicantNum: 0

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========   ==== ==== ============== ================= =============== ========
sa1         1    D    00d0.59ab.7037 Authenticated     --              test1
```

Related Commands show dot1x supplicant

undebug dot1x

Overview This command applies the functionality of the **no** variant of the debug dot1x command.

30 Authentication Commands

Introduction

Overview This chapter provides an alphabetical reference for authentication commands.

Command List

auth auth-fail vlan

Overview Use this command to enable the **auth-fail vlan** feature on the specified vlan interface. This feature assigns supplicants (client devices) to the specified VLAN if they fail port authentication.

Use the **no** variant of this command to disable the auth-fail vlan feature for a specified VLAN interface.

Syntax

```
auth auth-fail vlan <1-4094>
no auth auth-fail vlan
```

Parameter	Description
<1-4094>	Assigns the VLAN ID to any supplicants that have failed port authentication.

Default The auth-fail vlan feature is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Use the auth-fail vlan feature when using Web-Authentication instead of the Guest VLAN feature, when you need to separate networks where one supplicant (client device) requires authentication and another supplicant does not require authentication from the same interface.

This is because the DHCP lease time using the Web-Authentication feature is shorter, and the auth-fail vlan feature enables assignment to a different VLAN if a supplicant fails authentication.

To enable the auth-fail vlan feature with Web Authentication, you need to set the Web Authentication Server virtual IP address by using the auth-web-server ipaddress command or the auth-web-server dhcp ipaddress command.

When using 802.1X port authentication, use a dot1x max-auth-fail command to set the maximum number of login attempts. Three login attempts are allowed by default for 802.1X port authentication before supplicants trying to authenticate are moved from the Guest VLAN to the auth-fail VLAN. See the dot1x max-auth-fail on page 1100 for command information.

See the Authentication Feature Overview and Configuration Guide for information about:

- the auth-fail VLAN feature, which allows the Network Administrator to separate the supplicants who attempted authentication, but failed, from the supplicants who did not attempt authentication, and
- restrictions regarding combinations of authentication enhancements working together

Use appropriate ACLs (Access Control Lists) on interfaces for extra security if a supplicant allocated to the designated auth-fail vlan can access the same network

as a supplicant on the Guest VLAN. For more information about ACL concepts, and configuring ACLs see the ACL Feature Overview and Configuration Guide. For more information about ACL commands see:

Examples To enable the auth-fail vlan feature for port1.0.2 and assign VLAN 100, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth auth-fail vlan 100
```

To disable the auth-fail vlan feature for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth auth-fail vlan
```

To enable the auth-fail vlan feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth auth-fail vlan 100
```

To disable the auth-fail vlan feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth auth-fail vlan
```

Related Commands

auth profile (Global Configuration)

dot1x max-auth-fail

show dot1x

show dot1x interface

show running-config

auth critical

Overview This command enables the critical port feature on the interface. When the critical port feature is enabled on an interface, and all the RADIUS servers are unavailable, then the interface becomes authorized.

The **no** variant of this command disables critical port feature on the interface.

Syntax

```
auth critical
no auth critical
```

Default The critical port of port authentication is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable the critical port feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth critical
```

To disable the critical port feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth critical
```

To enable the critical port feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth critical
```

To disable the critical port feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth critical
```

Related Commands

auth profile (Global Configuration)

show auth-web-server

show dot1x

show dot1x interface

show running-config

auth dynamic-vlan-creation

Overview This command enables and disables the Dynamic VLAN assignment feature.

The Dynamic VLAN assignment feature allows a supplicant (client device) to be placed into a specific VLAN based on information returned from the RADIUS server during authentication, on a given interface.

Use the **no** variant of this command to disable the Dynamic VLAN assignment feature.

Syntax

```
auth dynamic-vlan-creation [rule {deny|permit}] [type
{multi|single}]
```

```
no auth dynamic-vlan-creation
```

Parameter	Description
`rule`	VLAN assignment rule.
`deny`	Deny a differently assigned VLAN ID. This is the default rule.
`permit`	Permit a differently assigned VLAN ID.
`type`	Specifies whether multiple different VLANs can be assigned to supplicants (client devices) attached to the port, or whether only a single VLAN can be assigned to supplicants on the port.
`multi`	Multiple Dynamic VLAN.
`single`	Single Dynamic VLAN.

Default By default, the Dynamic VLAN assignment feature is disabled.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage If the Dynamic VLAN assignment feature is enabled (disabled by default), VLAN assignment is dynamic. If the Dynamic VLAN assignment feature is disabled then RADIUS attributes are ignored and configured VLANs are assigned to ports. Dynamic VLANs may be associated with authenticated MAC addresses if the **type** parameter is applied with the **rule** parameter.

The **rule** parameter deals with the case where there are multiple supplicants attached to a port, and the type parameter has been set to **single-vlan**. The parameter specifies how the switch should act if different VLAN IDs end up being assigned to different supplicants. The keyword value **deny** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is rejected. The keyword value **permit** means that once a given VID has been assigned to the first supplicant, then if any subsequent supplicant is assigned a different VID, that supplicant is accepted, but it is actually assigned the same VID as the first supplicant.

If you issue an **auth dynamic-vlan-creation** command without a **rule** parameter then a second supplicant with a different VLAN ID is rejected. It is not assigned to the first supplicant's VLAN. Issuing an **auth dynamic-vlan-creation** command without a **rule** parameter has the same effect as issuing an **auth dynamic-vlan-creation rule deny** command rejecting supplicants with differing VIDs.

The **type** parameter specifies whether multiple different VLANs can be assigned to supplicants attached to the port, or whether only a single VLAN can be assigned to supplicants on the port. The **type** parameter can select the port base VLAN or the MAC base VLAN from the RADIUS VLAN ID. This can be used when the host-mode is set to multi-supplicant. For **single**-host ports, the VLAN ID will be assigned to the port. It is not supported with the Guest VLAN feature. Display the ID assigned using a **show vlan** command. For **multi**-host ports, the VLAN ID will be assigned to the MAC address of the authenticated supplicant. The VLAN ID assigned for the MAC Base VLAN is displayed using the **show platform table vlan** command.

To configure Dynamic Vlan with Web Authentication, you need to set Web Authentication Server virtual IP address by using the auth-web-server ipaddress command or the auth-web-server dhcp ipaddress command. You also need to create a hardware access-list that can be applied to the switch port interface.

You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

Examples To enable the Dynamic VLAN assignment feature on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport access vlan 10
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# interface vlan10
awplus(config-if)# ip address 10.1.1.1/24
```

To enable the Dynamic VLAN assignment feature with Web Authentication on interface `port1.0.2` when Web Authentication is needed, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 1.2.3.4
awplus(config)# access-list hardware acl-web send-to-cpu ip any
1.2.3.4
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# access-group acl-web
awplus(config-if)# interface vlan1
awplus(config-if)# ip address 10.1.1.1/24
```

To disable the Dynamic VLAN assignment feature on interface `port1.0.2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth dynamic-vlan-creation
```

To enable the Dynamic VLAN assignment feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth dynamic-vlan-creation
```

To disable the Dynamic VLAN assignment feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth dynamic-vlan-creation
```

Validation Commands

show dot1x

show dot1x interface

show running-config

Related Commands

auth profile (Global Configuration)

auth host-mode

auth guest-vlan

Overview This command enables and configures the Guest VLAN feature on the interface specified by associating a Guest VLAN with an interface. This command does not start authentication. The supplicant's (client device's) traffic is associated with the native VLAN of the interface if its not already associated with another VLAN. The **routing** option enables routing from the Guest VLAN to another VLAN, so the switch can lease DHCP addresses and accept access to a limited network.

The **no** variant of this command disables the guest VLAN feature on the interface specified.

Syntax

```
auth guest-vlan <1-4094> [routing]
no auth guest-vlan [routing]
```

Parameter	Description
<1-4094>	VLAN ID (VID).
`routing`	Enables routing from the Guest VLAN to other VLANs.

Default The Guest VLAN authentication feature is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage The Guest VLAN feature may be used by supplicants (client devices) that have not attempted authentication, or have failed the authentication process. Note that if a port is in multi-supplicant mode with per-port dynamic VLAN configuration, after the first successful authentication, subsequent hosts cannot use the guest VLAN due to the change in VLAN ID. This may be avoided by using per-user dynamic VLAN assignment.

When using the Guest VLAN feature with the multi-host mode, a number of supplicants can communicate via a guest VLAN before authentication. A supplicant's traffic is associated with the native VLAN of the specified switch port. The supplicant must belong to a VLAN before traffic from the supplicant can be associated.

Note that you must enable 802.1X on the port and define a VLAN using the vlan command before you can configure it as a guest VLAN.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

The Guest VLAN feature in previous releases had some limitations that have been removed. Until this release the Guest VLAN feature could not lease the IP address to the supplicant using DHCP Server or DHCP Relay features unless Web-Authentication was also applied. When using NAP authentication, the supplicant should have been able to log on to a domain controller to gain certification, but the Guest VLAN would not accept access to another VLAN.

The Guest VLAN routing mode in this release overcomes these issues. With the Guest VLAN routing mode, the switch can lease DHCP addresses and accept access to a limited network.

Note that Guest VLAN can use only untagged ports.

See the Authentication Feature Overview and Configuration Guide for information about:

- Guest VLAN, and
- restrictions regarding combinations of authentication enhancements working together

Examples To define vlan100 and assign the guest VLAN feature to vlan100 on interface port1.0.2, and enable routing from the guest VLAN to other VLANs, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth guest-vlan 100 routing
```

To disable the guest VLAN feature on port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan
```

To define vlan100 and assign the guest VLAN feature to vlan100 on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 100
awplus(config-vlan)# exit
awplus(config)# auth profile student
awplus(config-auth-profile)# auth guest-vlan 100
```

To disable the guest VLAN feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth guest-vlan
```

Related Commands auth profile (Global Configuration)

auth guest-vlan forward

Overview Use this command to enable packet forwarding from the Guest VLAN to a destination IP address or subnet. If this command is configured, the device can lease DHCP addresses and accept access to a limited part of your network. Also, when using NAP authentication, the supplicant can log on to a domain controller to gain certification.

Use the **no** variant of this command to disable packet forwarding from the Guest VLAN to a destination IP address or subnet.

Syntax

```
auth guest-vlan forward {<ip-address>|<ip-address/mask>}
[dns|tcp <1-65535>|udp <1-65535>]
```

```
no auth guest-vlan forward {<ip-address>|<ip-address/mask>}
[dns|tcp <1-65535>|udp <1-65535>]
```

Parameter	Description
<ip-address> <ip-address/mask>	The IP address or subnet to which the guest VLAN can forward packets, in dotted decimal notation
`dns`	Enable forwarding of DNS packets
`tcp <1-65535>`	Enable forwarding of packets for the specified TCP port number
`udp <1-65535>`	Enable forwarding of packets for the specified UDP port number

Default Forwarding is disabled by default.

Mode Interface Configuration mode for a specified switch port, or Authentication Profile mode

Usage Before using this command, you must configure the guest VLAN with the auth guest-vlan command.

Example To enable packet forwarding from the guest VLAN to the destination IP address on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth guest-vlan forward 10.0.0.1
```

To enable forwarding of DNS packets from the guest VLAN to the destination IP address on interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth guest-vlan forward 10.0.0.1 dns
```

To disable forwarding of DNS packets from the guest VLAN to the destination IP address on port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth guest-vlan forward 10.0.0.1 dns
```

To enable the tcp forwarding port 137 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth guest-vlan forward 10.0.0.1
tcp 137
```

To disable the tcp forwarding port 137 authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth guest-vlan forward
10.0.0.1 tcp 137
```

Related Commands

auth guest-vlan

auth profile (Global Configuration)

show running-config

auth host-mode

Overview This command selects host mode on the interface. Multi-host is an extension to IEEE802.1X.

Use the **no** variant of this command to set host mode to the default setting (single host).

Syntax

```
auth host-mode {single-host|multi-host|multi-supplicant}
no auth host-mode
```

Parameter	Description
`single-host`	Single host mode. In this mode, only one host may be authorized with the port. If other hosts out the interface attempt to authenticate, the authenticator blocks the attempt.
`multi-host`	Multi host mode. In this mode, multiple hosts may be authorized with the port; however only one host must be successfully authenticated at the Authentication Server for all hosts to be authorized with the port. Upon one host being successfully authenticated (state Authenticated), the other hosts will be automatically authorized at the port (state ForceAuthorized). If no host is successfully authenticated, then all hosts are not authorized with the port.
`multi-supplicant`	Multi supplicant (client device) mode. In this mode, multiple hosts may be authorized with the port, but each host must be individually authenticated with the Authentication Server to be authorized with the port. Supplicants which are not authenticated are not authorized with the port, while supplicants which are successfully authenticated are authorized with the port.

Default The default host mode for port authentication is for a single host.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Ports residing in the unauthorized state for host(s) or supplicant(s), change to an authorized state when the host or supplicant has successfully authenticated with the Authentication Server.

When multi-host mode is used or auth critical feature is used, all hosts do not need to be authenticated.

Examples

To set the host mode to multi-supplicant on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth host-mode multi-supplicant
```

To set the host mode to default (single host) on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth host-mode
```

To set the host mode to multi-supplicant on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth host-mode multi-supplicant
```

To set the host mode to default (single host) on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth host-mode
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show running-config

auth log

Overview Use this command to configure the types of authentication feature log messages that are output to the log file.

Use the **no** variant of this command to remove either specified types or all types of authentication feature log messages that are output to the log file.

Syntax

```
auth log {dot1x|auth-mac|auth-web}
{success|failure|logoff|all}
```

```
no auth log {do1x|auth-mac|auth-web}
{success|failure|logoff|all}
```

Parameter	Description
`dot1x`	Specify only 802.1X-Authentication log messages are output to the log file.
`auth-mac`	Specify only MAC-Authentication log messages are output to the log file.
`auth-web`	Specify only Web-Authentication log messages are output to the log file.
`success`	Specify only successful authentication log messages are output to the log file.
`failure`	Specify only authentication failure log messages are output to the log file.
`logoff`	Specify only authentication log-off messages are output to the log file. Note that link down, age out and expired ping polling messages will be included.
`all`	Specify all types of authentication log messages are output to the log file Note that this is the default behavior for the authentication logging feature.

Default All types of authentication log messages are output to the log file by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To configure the logging of MAC authentication failures to the log file for supplicants (client devices) connected to interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth log auth-mac failure
```

To disable the logging of all types of authentication log messages to the log file for supplicants (client devices) connected to interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth log all
```

To configure the logging of web authentication failures to the log file for supplicants (client devices) connected to authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth log auth-web failure
```

To disable the logging of all types of authentication log messages to the log file for supplicants (client devices) connected to authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth log all
```

Related Commands

auth profile (Global Configuration)

show running-config

auth max-supplicant

Overview This command sets the maximum number of supplicants (client devices) that can be authenticated on the selected port. Once this value is exceeded, further supplicants will not be authenticated.

The **no** variant of this command resets the maximum supplicant number to the default.

Syntax

```
auth max-supplicant <2-1024>
no auth max-supplicant
```

Parameter	Description
<2-1024>	Limit number.

Default The max supplicant of port authentication is 1024.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the maximum number of supplicants to `10` on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth max-supplicant 10
```

To reset the maximum number of supplicant to default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth max-supplicant
```

To set the maximum number of supplicants to 10 on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth max-supplicant 10
```

To reset the maximum number of supplicant to default on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth max-supplicant
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show running-config

auth profile (Global Configuration)

Overview Use this command to enter port authentication profile mode and configure a port authentication profile.

If the specified profile does not exist a new authentication profile is created with the name provided.

Use the **no** variant of this command to delete the specified port authentication profile.

Syntax

```
auth profile <profile-name>
no auth profile <profile-name>
```

Parameter	Description
<varname>	Name of the profile to create or configure.

Default No port authentication profiles are created by default.

Mode Global Configuration

Usage A port authentication profile is a configuration object that aggregates multiple port authentication commands. These profiles are attached or detached from an interface using the auth profile (Interface Configuration) command.

Example To create a new authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)#
```

To delete an authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# no auth profile student
```

Related Commands auth profile (Interface Configuration)

description (Authentication Profile)

auth profile (Interface Configuration)

Overview Use this command to attach a port authentication profile to the current interface.

Use the **no** variant of this command to detach a port authentication profile from the current interface.

Syntax

```
auth profile <profile-name>
no auth profile <profile-name>
```

Parameter	Description
<profile-name>	The name of the profile to attach to the current interface.

Default No profile is attached by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port.

Usage This command attaches a authentication profile, created using the auth profile (Global Configuration) command, to a static channel, a dynamic (LACP) channel group, or a switch port.

You can only attach one profile to an interface at a time, use the **no** variant of the command to detach a profile before attempting to attach another one.

Example To attach the authentication profile 'student' to port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# auth profile student
```

To detach the authentication profile 'student' from port1.0.1, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no auth profile student
```

Related Commands auth profile (Global Configuration)

auth reauthentication

Overview This command enables re-authentication on the interface specified in the Interface mode, which may be a static channel group (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the **no** variant of this command to disables reauthentication on the interface.

Syntax

```
auth reauthentication
no auth reauthentication
```

Default Reauthentication of port authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable reauthentication on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth reauthentication
```

To disable reauthentication on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth reauthentication
```

To enable reauthentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth reauthentication
```

To disable reauthentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth reauthentication
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show running-config

auth roaming disconnected

Overview This command allows a supplicant to move to another authenticating interface without reauthentication, even if the link is down for the interface that the supplicant is currently connected to.

You must enter the auth roaming enable command on both interfaces before using this command.

The **no** variant of this command disables roaming authentication on interfaces that are link-down, and forces a supplicant to be reauthenticated when moving between interfaces.

See the Authentication Feature Overview and Configuration Guide for further information about this feature.

Syntax

```
auth roaming disconnected
no auth roaming disconnected
```

Default By default, the authentication status for a roaming supplicant is deleted when an interface goes down, so supplicants must reauthenticate.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Note that 802.1X port authentication, MAC-authentication, or Web-authentication must be configured before using this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

Examples To allow supplicants to move from port1.0.2 without reauthentication even when the link is down, when using 802.1X authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
awplus(config-if)# auth roaming disconnected
```

To require supplicants to reauthenticate when moving from port1.0.2 if the link is down, when using 802.1X authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth roaming disconnected
```

To allow supplicants using authentication profile 'student' to move between ports without reauthentication even when the link is down, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth roaming disconnected
```

To require supplicants using authentication profile 'student' to reauthenticate when moving between ports if the link is down, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth roaming disconnected
```

Related Commands

auth profile (Global Configuration)

auth-mac enable

auth roaming enable

auth-web enable

dot1x port-control

show auth interface

show dot1x interface

show running-config

auth roaming enable

Overview This command allows a supplicant to move to another authenticating interface without reauthentication, providing the link is up for the interface that the supplicant is is currently connected to.

The **no** variant of this command disables roaming authentication on an interface, and forces a supplicant to be reauthenticated when moving between interfaces.

See the Authentication Feature Overview and Configuration Guide for further information about this feature.

Syntax

```
auth roaming enable
no auth roaming enable
```

Default Roaming authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Note that 802.1X port authentication, MAC-authentication, or Web-authentication must be configured before using this feature. The port that the supplicant is moving to must have the same authentication configuration as the port the supplicant is moving from.

This command only enables roaming authentication for links that are up. If you want roaming authentication on links that are down, you must also use the command auth roaming disconnected.

Roaming Authentication cannot be enabled if DHCP snooping is enabled (service dhcp-snooping command), and vice versa.

Examples To enable roaming authentication for port1.0.4, when using 802.1X authentication, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth roaming enable
```

To disable roaming authentication for port1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.4
awplus(config-if)# no auth roaming enable
```

To enable roaming authentication for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth roaming enable
```

To disable roaming authentication for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth roaming enable
```

Related Commands

auth profile (Global Configuration)

auth-mac enable

auth roaming disconnected

auth-web enable

dot1x port-control

show auth interface

show dot1x interface

show running-config

auth supplicant-ip

Overview This command adds a supplicant (client device) IP address on a given interface and provides parameters for its configuration.

Use the **no** variant of this command to delete the supplicant IP address and reset other parameters to their default values. The IP address can be determined before authentication for only auth-web client.

Syntax

```
auth supplicant-ip <ip-addr> [max-reauth-req <1-10>]
[port-control {auto|force-authorized|force-unauthorized}]
[quiet-period <1-65535>] [reauth-period <1-4294967295>]
[supp-timeout <1-65535>] [server-timeout <1-65535>]
[reauthentication]
```

```
no auth supplicant-ip <ip-addr> [reauthentication]
```

Parameter	Description
<ip-addr>	IP address of the supplicant entry in A.B.C.D/P format.
max-reauth-req	The number of reauthentication attempts before becoming unauthorized.
<1-10>	Count of reauthentication attempts (default 2).
port-control	Port control commands.
auto	A port control parameter that allows port clients to negotiate authentication.
force-authorized	A port control parameter that forces the port state to authorized.
force-unauthorized	A port control parameter that forces the port state to unauthorized.
quiet-period	Quiet period during which the port remains in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
reauth-period	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).
supp-timeout	Supplicant response timeout.
<1-65535>	Seconds for supplicant response timeout (default 30 seconds).
server-timeout	The period, in seconds, before the authentication server response times out.
<1-65535>	The server-timeout period, in seconds, default 3600 seconds.
reauthentication	Enable reauthentication on a port.

Default No supplicant IP address for port authentication exists by default until first created with the **auth supplicant-ip** command. The defaults for parameters applied are as shown in the table above.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, a switch port, or Auth Profile.

Examples To add the supplicant IP address 192.168.10.0/24 to force authorized port control for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-ip 192.168.10.0/24
port-control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
```

To disable reauthentication for the supplicant(s) IP address 192.168.10.0/24 for interface port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
reauthentication
```

To add the supplicant IP address 192.168.10.0/24 to force authorized port control for auth profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth supplicant-ip
192.168.10.0/24 port-control force-authorized
```

To delete the supplicant IP address 192.168.10.0/24 for auth profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth supplicant-ip
192.168.10.0/24
```

To disable reauthentication for the supplicant IP address 192.168.10.0/24, for auth profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-if)# no auth supplicant-ip 192.168.10.0/24
reauthentication
```

Validation Commands

show auth

show dot1x

show dot1x interface

show running-config

auth supplicant-mac

Overview This command adds a supplicant (client device) MAC address or MAC mask on a given interface with the parameters as specified in the table below.

Use the **no** variant of this command to delete the supplicant MAC address and reset other parameters to their default values.

Syntax

```
auth supplicant-mac <mac-addr> [mask <mac-addr-mask>]
[max-reauth-req <1-10>] [port-control
{auto|force-authorized|force-unauthorized|skip-second-auth}]
[quiet-period <1-65535>] [reauth-period <1-4294967295>]
[supp-timeout <1-65535>] [server-timeout <1-65535>]
[reauthentication]
```

```
no auth supplicant-mac <mac-addr> [reauthentication]
```

Parameter	Description
<mac-addr>	MAC (hardware) address of the supplicant entry in HHHH.HHHH.HHHH MAC address hexadecimal format.
`mask`	A mask applied to MAC addresses in order to select only those addresses containing a specific string.
<mac-addr-mask>	The mask comprises a string of three (period separated) bytes, where each byte comprises four hexadecimal characters that will generally be either 1or 0. When the mask is applied to a specific MAC address, a match is only required for characters that correspond to a 1 in the mask. Characters that correspond to a 0 in the mask are effectively ignored. In the examples section below, the mask ffff.ff00.0000 is applied for the MAC address 0000.5E00.0000. The applied mask will then match only those MAC addresses that begin with 0000.5E (in this case the OUI component). The remaining portion of the addresses (in this case the NIC component) will be ignored.
`port-control`	Port control commands.
`auto`	Allow port client to negotiate authentication.
`force-authorized`	Force port state to authorized.
`force-unauthorized`	Force port state to unauthorized.
`skip-second-auth`	Skip the second authentication.
`quiet-period`	Quiet period in the HELD state (default 60 seconds).
<1-65535>	Seconds for quiet period.
`reauth-period`	Seconds between reauthorization attempts (default 3600 seconds).
<1-4294967295>	Seconds for reauthorization attempts (reauth-period).

Parameter	Description
`supp-timeout`	Supplicant response timeout (default 30 seconds).
<1-65535>	Seconds for supplicant response timeout.
`server-timeout`	Authentication server response timeout (default 30 seconds).
<1-65535>	Seconds for authentication server response timeout.
`reauthentication`	Enable reauthentication on a port.
`max-reauth-req`	No of reauthentication attempts before becoming unauthorized (default 2).
<1-10>	Count of reauthentication attempts.

Default No supplicant MAC address for port authentication exists by default until first created with the **auth supplicant-mac** command. The defaults for parameters are shown in the table above.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To add the supplicant MAC address 0000.5E00.5343 to force authorized port control for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-mac 0000.5E00.5343
port-control force-authorized
```

To apply the mask ffff.ff00.0000 in order to add any supplicant whose MAC address begins with 000.5E, and then to force authorized port control for port 1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth supplicant-mac 0000.5E00.0000 mask
ffff.ff00.0000 port-control force-authorized
```

To delete the supplicant MAC address 0000.5E00.5343 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0000.5E00.5343
```

To reset reauthentication to disabled for the supplicant MAC address 0000.5E00.5343 for port1.0.2, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth supplicant-mac 0000.5E00.5343
reauthentication
```

To add the supplicant MAC address 0000.5E00.5343 to force authorized port control for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth supplicant-mac
0000.5E00.5343 port-control force-authorized
```

To delete the supplicant MAC address 0000.5E00.5343 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth supplicant-mac
0000.5E00.5343
```

To disable reauthentication for the supplicant MAC address 0000.5E00.5343 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth supplicant-mac
0000.5E00.5343 reauthentication
```

Related Commands

show auth

show dot1x

show dot1x interface

show running-config

auth timeout connect-timeout

Overview This command sets the connect-timeout period for the interface.

Use the **no** variant of this command to reset the connect-timeout period to the default.

Syntax

```
auth timeout connect-timeout <1-65535>
no auth timeout connect-timeout
```

Parameter	Description
<1-65535>	Specifies the connect-timeout period (in seconds).

Default The connect-timeout default is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage This command is used for MAC- and Web-Authentication. If the connect-timeout has lapsed and the supplicant has the state **connecting**, then the supplicant is deleted. When auth-web-server session-keep or auth two-step enableis enabled, we recommend you configure a longer connect-timeout period.

Examples To set the connect-timeout period to 3600 seconds for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout connect-timeout 3600
```

To reset the connect-timeout period to the default (30 seconds) for port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout connect-timeout
```

To set the connect-timeout period to 3600 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout connect-timeout 3600
```

To reset the connect-timeout period to the default (30 seconds) for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout connect-timeout
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

auth timeout quiet-period

Overview This command sets a time period for which another authentication request is not accepted on a given interface, after an authentication request has failed.

Use the **no** variant of this command to reset the quiet period to the default.

Syntax

```
auth timeout quiet-period <1-65535>
no auth timeout quiet-period
```

Parameter	Description
<1-65535>	Specifies the quiet period (in seconds).

Default The quiet period for port authentication is 60 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the quiet period to 10 seconds for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout quiet-period
```

To set the quiet period to 10 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout quiet-period 10
```

To reset the quiet period to the default (60 seconds) for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout quiet-period
```

Related Commands auth profile (Global Configuration)

auth timeout reauth-period

Overview This command sets the timer for reauthentication on a given interface. The re-authentication for the supplicant (client device) is executed at this timeout. The timeout is only applied if the **auth reauthentication** command is applied.

Use the **no** variant of this command to reset the **reauth-period** parameter to the default (3600 seconds).

Syntax

```
auth timeout reauth-period <1-4294967295>
no auth timeout reauth-period
```

Parameter	Description
<1-4294967295>	The reauthentication timeout period (in seconds).

Default The default reauthentication period for port authentication is 3600 seconds, when reauthentication is enabled on the port.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the reauthentication period to 1 day for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout reauth-period
```

To set the reauthentication period to 1 day for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout reauth-period 86400
```

To reset the reauthentication period to the default (3600 seconds) for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout reauth-period
```

Related Commands

auth profile (Global Configuration)

auth reauthentication

show dot1x

show dot1x interface

show running-config

auth timeout server-timeout

Overview This command sets the timeout for the waiting response from the RADIUS server on a given interface.

The **no** variant of this command resets the server-timeout to the default (30 seconds).

Syntax

```
auth timeout server-timeout <1-65535>
no auth timeout server-timeout
```

Parameter	Description
<1-65535>	Server timeout period (in seconds).

Default The server timeout for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the server timeout to 120 seconds for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout server-timeout
```

To set the server timeout to 120 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout server-timeout 120
```

To set the server timeout to the default (30 seconds) for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout server-timeout
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show running-config

auth timeout supp-timeout

Overview This command sets the timeout of the waiting response from the supplicant (client device) on a given interface.

The **no** variant of this command resets the supplicant timeout to the default (30 seconds).

Syntax

```
auth timeout supp-timeout <1-65535>
no auth timeout supp-timeout
```

Parameter	Description
<1-65535>	The sup-timeout period (in seconds).

Default The supplicant timeout for port authentication is 30 seconds.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the server timeout to 2 seconds for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth timeout supp-timeout 2
```

To reset the server timeout to the default (30 seconds) for interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth timeout supp-timeout
```

To set the server timeout to 2 seconds for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth timeout supp-timeout 2
```

To reset the server timeout to the default (30 seconds) for authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth timeout supp-timeout
```

Related Commands

auth profile (Global Configuration)

show dot1x

show dot1x interface

show running-config

auth two-step enable

Overview This command enables a two-step authentication feature on an interface. When this feature is enabled, the supplicant is authorized in a two-step process. If authentication succeeds, the supplicant becomes authenticated. This command will apply the two-step authentication method based on 802.1X-, MAC- or Web-Authentication.

The **no** variant of this command disables the two-step authentication feature.

Syntax

```
auth two-step enable
no auth two-step enable
```

Default Two step authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage The single step authentication methods (either user or device authentication) have a potential security risk:

- an unauthorized user can access the network with an authorized device, or
- an authorized user can access the network with an unauthorized device.

Two-step authentication solves this problem by authenticating both the user and the device. The supplicant will only become authenticated if both these steps are successful. If the first authentication step fails, then the second step is not started.

Examples To enable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth two-step enable
```

To disable the two step authentication feature, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth two-step enable
```

To enable MAC-Authentication followed by 802.1X-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable MAC-Authentication followed by Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-mac enable
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable 802.1X-Authentication followed by Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# dot1x port-control auto
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth two-step enable
```

To enable the two step authentication feature for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth two-step enable
```

To disable the two step authentication feature for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth two-step enable
```

Validation Commands

show startup-config

show auth supplicant

show dot1x supplicant

Related Commands

auth profile (Global Configuration)

show auth two-step supplicant brief

show auth

show auth interface

show auth supplicant

show dot1x

show dot1x interface

show dot1x supplicant

auth-mac accounting

Overview This command overrides the **default** RADIUS accounting method for MAC-based authentication on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
auth-mac accounting {default|<list-name>}
no auth-mac accounting
```

Parameter	Description
default	Apply the default accounting method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Mode

Example To apply the named list 'vlan10_acct' on the `vlan10` interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-mac accounting vlan10_acct
```

To remove the named list from the `vlan10` interface and set the accounting method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-mac accounting
```

Related Commands aaa accounting auth-mac

auth-mac authentication

Overview This command overrides the **default** MAC-based authentication method on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
auth-mac authentication {default|<list-name>}
no auth-mac authentication
```

Parameter	Description
`default`	Apply the default authentication method list
<list-name>	Apply a user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Mode

Example To apply the named list 'vlan10_auth' on the `vlan10` interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-mac authentication vlan10_auth
```

To remove the named list from the `vlan10` interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-mac authentication
```

Related Commands aaa authentication auth-mac

auth-mac enable

Overview This command enables MAC-based authentication on the interface specified in the Interface command mode.

Use the **no** variant of this command to disable MAC-based authentication on an interface.

Syntax

```
auth-mac enable
no auth-mac enable
```

Default MAC-Authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Enabling **spanning-tree edgeport** on ports after enabling MAC-based authentication avoids unnecessary re-authentication when the port state changes, which does not happen when spanning tree edgeport is enabled. Note that re-authentication is correct behavior without **spanning-tree edgeport** enabled.

Applying **switchport mode access** on ports is also good practice to set the ports to access mode with ingress filtering turned on, whenever ports for MAC-Authentication are in a VLAN.

Examples To enable MAC-Authentication on interface `port1.0.2` and enable spanning tree edgeport to avoid unnecessary re-authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac enable
awplus(config-if)# spanning-tree edgeport
awplus(config-if)# switchport mode access
```

To disable MAC-Authentication on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac enable
```

To enable MAC authentication on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-mac enable
```

To disable MAC authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-mac enable
```

Related Commands

auth profile (Global Configuration)

show auth

show auth interface

show running-config

auth-mac method

Overview This command sets the type of authentication method for MAC-Authentication that is used with RADIUS on the interface specified in the Interface command mode.

The **no** variant of this command resets the authentication method used to the default method (PAP) as the RADIUS authentication method used by the MAC-Authentication.

Syntax

```
auth-mac method [eap-md5|pap]
no auth-mac method
```

Parameter	Description
`eap-md5`	Enable EAP-MD5 of authentication method.
`pap`	Enable PAP of authentication method.

Default The MAC-Authentication method is PAP.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the MAC-Authentication method to `pap` on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac method pap
```

To set the MAC-Authentication method to the default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-mac method
```

To enable MAC authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-mac enable
```

To disable MAC authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-mac enable
```

Related Commands

auth profile (Global Configuration)

show auth

show auth interface

show running-config

auth-mac password

Overview This command changes the password for MAC-based authentication.

Use the **no** variant of this command to return the password to its default.

Syntax

```
auth-mac [encrypted] password <password>
no auth-mac password
```

Parameter	Description
`auth-mac`	MAC-based authentication
`encrypted`	Specify an encrypted password
`password`	Configure the password
<password>	The new password. Passwords can be up to 64 characters in length and can contain any printable characters except • ? • " (double quotes) • space

Default By default, the password is the MAC address of the supplicant

Mode Global Configuration

Usage Changing the password increases the security of MAC-based authentication, because the default password is easy for an attacker to discover. This is particularly important if:

- some MAC-based supplicants on the network are intelligent devices, such as computers, and/or
- you are using two-step authentication (see the "Ensuring Authentication Methods Require Different Usernames and Passwords" section of the Authentication Feature Overview_and Configuration Guide).

Examples To change the password to verySecurePassword, use the commands:

```
awplus# configure terminal
awplus(config)# auth-mac password verySecurePassword
```

Validation Command show running-config

Related Commands auth two-step enable

show auth

auth-mac reauth-relearning

Overview This command sets the MAC address learning of the supplicant (client device) to re-learning for re-authentication on the interface specified in the Interface command mode.

Use the **no** variant of this command to disable the auth-mac re-learning option.

Syntax

```
auth-mac reauth-relearning
no auth-mac reauth-relearning
```

Default Re-learning for port authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To enable the re-authentication re-learning feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-mac reauth-relearning
```

To disable the re-authentication re-learning feature on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awpl us(config-if)# no auth-mac reauth-relearning
```

To enable the re-authentication re-learning feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-mac reauth-relearning
```

To disable the re-authentication re-learning feature on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-mac reauth-relearning
```

Related Commands

auth profile (Global Configuration)

show auth

show auth interface

show running-config

auth-mac username

Overview Use this command to specify the format of the MAC address in the username and password field when a request for MAC-based authorization is sent to a RADIUS server.

Syntax

```
auth-mac username {ietf|unformatted} {lower-case|upper-case}
```

Parameter	Description
`ietf`	The MAC address includes a hyphen between each 2 bytes. (Example: xx-xx-xx-xx-xx-xx)
`unformatted`	The MAC address does not include hyphens. (Example: xxxxxxxxxxxx)
`lower-case`	The MAC address uses lower-case characters (a-f)
`upper-case`	The MAC address uses upper-case characters (A-F)

Default

```
auth-mac username ietf lower-case
```

Mode Global Configuration

Usage This command is provided to allow other vendors', AlliedWare, and AlliedWare Plus switches to share the same format on the RADIUS server.

Example To configure the format of the MAC address in the username and password field to be changed to IETF and upper-case, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-mac username ietf upper-case
```

Related Commands

auth-mac username

show running-config

auth-web accounting

Overview This command overrides the **default** RADIUS accounting method for Web-based authentication on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
auth-web accounting {default|<list-name>}
no auth-web accounting
```

Parameter	Description
default	Apply the default accounting method list
<list-name>	Apply a named accounting method list

Default The **default** method list is applied to an interface by default.

Mode Interface Mode

Example To apply the named list vlan10_acct' on the `vlan10` interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-web accounting vlan10_acct
```

To remove the named list from the `vlan10` interface and set the accounting method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-web accounting
```

Related Commands aaa accounting auth-web

auth-web authentication

Overview This command overrides the **default** Web-based authentication method on an interface by allowing you to apply a user-defined named list.

Use the **no** variant of this command to remove the named list from the interface and apply the **default** method.

Syntax

```
auth-web authentication {default|<list-name>}
no auth-web authentication
```

Parameter	Description
default	Apply the default authentication method list
<list-name>	Apply the user-defined named list

Default The **default** method list is applied to an interface by default.

Mode Interface Mode

Example To apply the named list 'vlan10_auth' on the `vlan10` interface, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# auth-web authentication vlan10_auth
```

To remove the named list from the `vlan10` interface and set the authentication method back to **default**, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no auth-web authentication
```

Related Commands aaa authentication auth-web

auth-web enable

Overview This command enables Web-based authentication in Interface mode on the interface specified.

Use the **no** variant of this command to apply its default.

Syntax

```
auth-web enable
no auth-web enable
```

Default Web-Authentication is disabled by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage Web-based authentication cannot be enabled if DHCP snooping is enabled by using the service dhcp-snooping command, and vice versa. You need to configure an IPv4 address for the VLAN interface on which Web Authentication is running.

Examples To enable Web-Authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# auth-web enable
```

To disable Web-Authentication on static-channel-group 2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# no auth-web enable
```

To enable Web authentication on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web enable
```

To disable Web authentication on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web enable
```

Related Commands

auth profile (Global Configuration)

show auth

show auth interface

show running-config

auth-web forward

Overview This command enables the Web-authentication packet forwarding feature on the interface specified. This command also enables ARP forwarding, and adds forwarded packets to the **tcp** or **udp** port number specified.

The **no** variant of this command disables the specified packet forwarding feature on the interface.

Syntax

```
auth-web forward [<ip-address>|<ip-address/prefix-length>]
{dns|tcp <1-65535>|udp <1-65535>}
```

Or

```
auth-web forward {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}
```

The **no** variant of this command are:

```
no auth-web forward [<ip-address>|<ip-address/prefix-length>]
{dns|tcp <1-65535>|udp <1-65535>}
```

Or

```
no auth-web forward {arp|dhcp|dns|tcp <1-65535>|udp <1-65535>}
```

Parameter	Description
<ip-address> <ip-address/ prefix-length>	The IP address or subnet on which the Web-authentication is to be enabled.
arp	Enable forwarding of ARP.
dhcp	Enable forwarding of DHCP (67/udp).
dns	Enable forwarding of DNS (53/udp).
tcp	Enable forwarding of TCP specified port number.
<1-65535>	TCP Port number.
udp	Enable forwarding of UDP specified port number.
<1-65535>	UDP Port number.

Default Packet forwarding for port authentication is enabled by default for “arp”, “dhcp” and “dns”.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Usage For more information about the *<ip-address>* parameter, and an example, see the “auth- web forward” section in the Alliedware Plus Technical Tips and Tricks.

Examples To enable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward arp
```

To add the TCP forwarding port 137 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web forward tcp 137
```

To add the DNS Server IP address 192.168.1.10 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# switchport mode access
awplus(config-if)# auth-web enable
awplus(config-if)# auth dynamic-vlan-creation
awplus(config-if)# auth-web forward 192.168.1.10 dns
```

To disable the ARP forwarding feature on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward arp
```

To delete the TCP forwarding port 137 on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp 137
```

To delete the all of TCP forwarding on interface port1.0.2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web forward tcp
```

To enable the arp forwarding feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web forward arp
```

To add the tcp forwarding port 137 on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web forward tcp 137
```

To disable the ARP forwarding feature on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web forward arp
```

To delete the tcp forwarding port 137 on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web forward tcp 137
```

To delete all tcp forwarding on authentication profile ‘student’, use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web forward tcp
```

Related Commands

auth profile (Global Configuration)

show auth

show auth interface

auth-web max-auth-fail

Overview This command sets the number of authentication failures allowed before rejecting further authentication requests. When the supplicant (client device) fails more than the specified number of times, then login requests are refused during the quiet period.

The **no** variant of this command resets the maximum number of authentication failures to the default.

Syntax

```
auth-web max-auth-fail <0-10>
no auth-web max-auth-fail
```

Parameter	Description
<0-10>	The maximum number of authentication requests allowed before failing.

Default The maximum number of authentication failures is set to 3.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Examples To set the lock count to `5` on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web max-auth-fail 5
```

To set the lock count to the default on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no auth-web max-auth-fail
```

To set the lock count to 5 on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web max-auth-fail 5
```

To set the lock count to the default on authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web max-auth-fail
```

Related Commands

auth profile (Global Configuration)

auth timeout quiet-period

show auth

show auth interface

show running-config

auth-web method

Overview This command sets the Web-authentication access method that is used with RADIUS on the interface specified.

The **no** variant of this command sets the authentication method to PAP for the interface specified when Web-Authentication is also used with the RADIUS authentication method.

Syntax

```
auth-web method {eap-md5|pap}
no auth-web method
```

Parameter	Description
`eap-md5`	Enable EAP-MD5 as the authentication method.
`pap`	Enable PAP as the authentication method.

Default The Web-Authentication method is set to PAP by default.

Mode Interface Configuration for a static channel, a dynamic (LACP) channel group, or a switch port; or Authentication Profile mode.

Example To set the Web-Authentication method to eap-md5 on interface `port1.0.2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# auth-web method eap-md5
```

To set the web authentication method to eap-md5 for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# auth-web method eap-md5
```

To reset the web authentication method to the default (PAP) for authentication profile 'student', use the commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no auth-web method
```

Related Commands

auth profile (Global Configuration)

show auth

show auth interface

show running-config

auth-web-server blocking-mode

Overview Use this command to enable blocking mode for the Web-Authentication server. The blocking mode displays an authentication success or failure screen immediately from the response result from a RADIUS server.

Use the **no** variant of this command to disable blocking mode for the Web-Authentication server.

Syntax
```
auth-web-server blocking-mode
no auth-web-server blocking-mode
```

Default By default, blocking mode is disabled for the Web-Authentication server.

Mode Global Configuration

Example To enable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server blocking-mode
```

To disable blocking mode for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server blocking-mode
```

Related Commands
auth-web-server redirect-delay-time

show auth-web-server

show running-config

auth-web-server dhcp ipaddress

Overview Use this command to assign an IP address and enable the DHCP service on the Web-Authentication server for supplicants (client devices).

Use the **no** variant of this command to remove an IP address and disable the DHCP service on the Web-Authentication server for supplicants.

Syntax

```
auth-web-server dhcp ipaddress <ip-address/prefix-length>
no auth-web-server dhcp ipaddress
```

Parameter	Description
<ip-addr/prefix-length>	The IPv4 address and prefix length assigned for the DHCP service on the Web-Authentication server for supplicants.

Default No IP address for the Web-Authentication server is set by default.

Mode Global Configuration

Usage See the Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

You cannot use the IPv4 address assigned to the device's interface as the Web-Authentication server address.

Examples To assign the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp ipaddress 10.0.0.1/8
```

To remove an IP address on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp ipaddress
```

Validation Commands show running-config

Related Commands show auth-web-server

auth-web-server dhcp lease

auth-web-server dhcp lease

Overview Use this command to set the DHCP lease time for supplicants (client devices) using the DHCP service on the Web-Authentication server.

Use the **no** variant of this command to reset to the default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server.

Syntax

```
auth-web-server dhcp lease <20-60>
no auth-web-server dhcp lease
```

Parameter	Description
<20-60>	DHCP lease time for supplicants using the DHCP service on the Web-Authentication server in seconds.

Default The default DHCP lease time for supplicants using the DHCP service on the Web-Authentication server is set to 30 seconds.

Mode Global Configuration

Usage See the Authentication Feature Overview and Configuration Guide for information about:

- using DHCP with web authentication, and
- restrictions regarding combinations of authentication enhancements working together

Examples To set the DHCP lease time to 1 minute for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp lease 60
```

To reset the DHCP lease time to the default setting (30 seconds) for supplicants using the DHCP service on the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server dhcp lease
```

Validation Commands show running-config

Related Commands show auth-web-server

auth-web-server dhcp ipaddress

auth-web-server dhcp-wpad-option

Overview This command sets the DHCP WPAD (Web Proxy Auto-Discovery) option for the Web-Authentication temporary DHCP service.

For more information and examples, see the "Web Auth Proxy" section in the Alliedware Plus Technical Tips and Tricks.

Use the **no** variant of this command to disable the DHCP WPAD function.

Syntax

```
auth-web-server dhcp wpad-option <url>
no auth-web-server dhcp wpad-option
```

Parameter	Description
<url>	URL to the server which gets a .pac file.

Default The Web-Authentication server DHCP WPAD option is not set.

Mode Global Configuration

Usage If the supplicant is configured to use WPAD, the supplicant's web browser will use TCP port 80 as usual. Therefore, the packet can be intercepted by Web-Authentication as normal, and the Web-Authentication Login page can be sent. However, after authentication, the browser does not know where to get the WPAD file and so cannot access external web pages. The WPAD file is usually named proxy.pac file and tells the browser what web proxy to use.

Use this command to tell the supplicant where it can get this file from. The switch itself can be specified as the source for this file, and it can deliver it to the supplicant on request.

Example To specify that the proxy.pac file is found on the server at 192.168.1.100, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server dhcp wpad-option
http://192.168.1.100/proxy/proxy.pac
```

Related Commands show auth-web-server

auth-web-server gateway (deleted)

Overview This command has been deleted from Software Version 5.4.4-2.3 and later, because it is no longer necessary to register the gateway information when the supplicant is authorized.

auth-web-server host-name

Overview This command assigns a hostname to the web authentication server.

Use the **no** variant of this command to remove the hostname from the web authentication server.

Syntax

```
auth-web-server host-name <hostname>
no auth-web-server host-name
```

Parameter	Description
<hostname>	URL string of the hostname

Default The web authentication server has no hostname.

Mode Global Configuration

Usage When the web authentication server uses HTTPS protocol, the web browser will validate the certificate. If the certificate is invalid, the web page gives a warning message before displaying server content. However, the web page will not give warning message if the server has a hostname same as the one stored in the installed certificate.

Examples To set the auth.example.com as the hostname of the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server host-name auth.example.com
```

To remove hostname auth.example.com from the web authentication server, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server host-name
```

Related Commands aaa authentication auth-web

auth-web enable

auth-web-server http-redirect (deleted)

Overview This command has been deleted in Software Version 5.4.4-2.3 and later, because the HTTP redirect feature is now always enabled and cannot be disabled.

auth-web-server intercept-port

Overview This command specifies any additional TCP port numbers that the Web-Authentication server is to intercept.

Use the **no** variant of this command to stop intercepting the TCP port numbers.

Syntax

```
auth-web-server intercept-port {<1-65535>|any}
no auth-web-server intercept-port {<1-65535>|any}
```

Parameter	Description
<1-65535>	TCP port number.
`any`	Intercept all TCP packets

Default No additional TCP port numbers are intercepted by default.

Mode Global Configuration

Usage If this command is not specified, AlliedWare Plus Web-Authentication intercepts the supplicant's initial TCP port 80 connection to a web page and sends it the Web-Authentication Login page. However, if the supplicant is configured to use a web proxy, then it will usually be using TCP port 8080 (or another user configured port number). In this case Web-Authentication cannot intercept the connection.

To overcome this limitation you can use this command to tell the switch which additional port it should intercept, and then send the Web-Authentication Login page to the supplicant.

When the web authentication switch is in a guest network, the switch does not know the proxy server's port number in the supplicant's proxy setting. To overcome this limitation, you can use the **any** option in this command to intercept all TCP packets.

When you use this command in conjunction with a proxy server configured in the web browser, you must add the proxy server's network as a 'No Proxy' network. You can specify 'No Proxy' networks in the proxy settings in your web browser. For more information, see the "Web Auth Proxy" section in the Alliedware Plus Technical Tips and Tricks.

Example To additionally intercept port number 3128, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server intercept-port 3128
```

Related Commands show auth-web-server

auth-web-server ipaddress

Overview This command sets the IP address for the Web-Authentication server.

Use the **no** variant of this command to delete the IP address for the Web-Authentication server.

You cannot use the IPv4 address assigned to the device's interface as the Web-Authentication server address.

Syntax

```
auth-web-server ipaddress <ip-address>
no auth-web-server ipaddress
```

Parameter	Description
<ip-address>	Web-Authentication server dotted decimal IP address in A.B.C.D format.

Default The Web-Authentication server address on the system is not set by default.

Mode Global Configuration

Examples To set the IP address `10.0.0.1` to the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ipaddress 10.0.0.1
```

To delete the IP address from the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ipaddress
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server page language

Overview Use this command to set the presentation language of Web authentication pages. Titles and subtitles of Web authentication pages will be set accordingly. Note that presently only English or Japanese are offered.

Use the **no** variant of this command to set the presentation language of Web authentication pages to its default (English).

Syntax

```
auth-web-server page language {english|japanese}
no auth-web-server page language
```

Parameter	Description
english	Web authentication pages are presented in English.
japanese	Web authentication pages are presented in Japanese.

Default Web authentication pages are presented in English by default.

Mode Global Configuration

Examples To set Japanese as the presentation language of Web authentication pages, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page language japanese
```

To set English as the presentation language of Web authentication pages, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page language english
```

To unset the presentation language of Web authentication pages and use English as the default presentation language, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page language
```

Related Commands

auth-web-server page title

auth-web-server page sub-title

show auth-web-server page

auth-web-server login-url

Overview This command sets the web-authentication login page URL.

Use the **no** variant of this command to delete the set URL.

Syntax

```
auth-web-server login-url <URL>
no auth-web-server login-url
```

Parameter	Description
<URL>	Set login page URL

Default The built-in login page is set by default.

Mode Global Configuration

Examples To set http://example.com/login.html as the login page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server login-url
http://example.com/login.html
```

To unset the login page URL, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server login-url
```

Related Commands show running-config

auth-web-server mode (deleted)

Overview This command has been deleted in Software Version 5.4.4-2.3 and later, because it is no longer necessary to configure an intercept mode.

auth-web-server page logo

Overview This command sets the type of logo that will be displayed on the web authentication page.

Use the **no** variant of this command to set the logo type to **auto**.

Syntax

```
auth-web-server page logo {auto|default|hidden}
no auth-web-server page logo
```

Parameter	Description
`auto`	Display the custom logo if installed; otherwise display the default logo
`default`	Display the default logo
`hidden`	Hide the logo

Default Logo type is **auto** by default.

Mode Global Configuration

Examples To display the default logo with ignoring installed custom logo, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page logo default
```

To set back to the default logo type **auto**, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page logo
```

Validation Commands show auth-web-server page

auth-web-server page sub-title

Overview This command sets the custom sub-title on the web authentication page.

Use the **no** variant of this command to reset the sub-title to its default.

Syntax

```
auth-web-server page sub-title {hidden|text <sub-title>}
no auth-web-server page sub-title
```

Parameter	Description
`hidden`	Hide the sub-title
<sub-title>	Text string of the sub-title

Default "Allied-Telesis" is displayed by default.

Mode Global Configuration

Examples To set the custom sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title text Web
Authentication
```

To hide the sub-title, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page sub-title hidden
```

To change back to the default title, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page sub-title
```

Validation Commands show auth-web-server page

auth-web-server page success-message

Overview This command sets the success message on the web-authentication page.

Use the **no** variant of this command to remove the success message.

Syntax

```
auth-web-server page success-message text <success-message>
no auth-web-server page success-message
```

Parameter	Description
<success-message>	Text string of the success message

Default No success message is set by default.

Mode Global Configuration

Examples To set the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page success-message text Your success message
```

To unset the success message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page success-message
```

Validation Commands show auth-web-server page

auth-web-server page title

Overview This command sets the custom title on the web authentication page.

Use the **no** variant of this command to remove the custom title.

Syntax

```
auth-web-server page title {hidden|text <title>}
no auth-web-server page title
```

Parameter	Description
`hidden`	Hide the title
<title>	Text string of the title

Default "Web Access Authentication Gateway" is displayed by default.

Mode Global Configuration

Examples To set the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title text Login
```

To hide the title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page title hidden
```

To unset the custom title on the web authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page title
```

Validation Commands show auth-web-server page

auth-web-server page welcome-message

Overview This command sets the welcome message on the web-authentication page.

Use the **no** variant of this command to remove the welcome message.

Syntax

```
auth-web-server page welcome-message text <welcome-message>
no auth-web-server page welcome-message
```

Parameter	Description
<welcome-message>	Text string of the welcome message

Default No welcome message is set by default.

Mode Global Configuration

Examples To set the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server page welcome-message text Your welcome message
```

To remove the welcome message on the web-authentication page, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server page welcome-message
```

Validation Commands show auth-web-server page

auth-web-server ping-poll enable

Overview This command enables the ping polling to the supplicant (client device) that is authenticated by Web-Authentication.

The **no** variant of this command disables the ping polling to the supplicant that is authenticated by Web-Authentication.

Syntax

```
auth-web-server ping-poll enable
no auth-web-server ping-poll enable
```

Default The ping polling feature for Web-Authentication is disabled by default.

Mode Global Configuration

Examples To enable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll enable
```

To disable the ping polling feature for Web-Authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll enable
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server ping-poll failcount

Overview This command sets a fail count for the ping polling feature when used with Web-Authentication. The **failcount** parameter specifies the number of unanswered pings. A supplicant (client device) is logged off when the number of unanswered pings are greater than the failcount set with this command.

Use the **no** variant of this command to resets the fail count for the ping polling feature to the default (5 pings).

Syntax

```
auth-web-server ping-poll failcount <1-100>
no auth-web-server ping-poll failcount
```

Parameter	Description
<1-100>	Count.

Default The default failcount for ping polling is 5 pings.

Mode Global Configuration

Examples To set the failcount of ping polling to `10` pings, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll failcount 10
```

To set the failcount of ping polling to default, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll failcount
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server ping-poll interval

Overview This command is used to change the ping poll interval. The interval specifies the time period between pings when the supplicant (client device) is reachable.

Use the **no** variant of this command to reset to the default period for ping polling (30 seconds).

Syntax

```
auth-web-server ping-poll interval <1-65535>
no auth-web-server ping-poll interval
```

Parameter	Description
<1-65535>	Seconds.

Default The interval for ping polling is 30 seconds by default.

Mode Global Configuration

Examples To set the interval of ping polling to `60` seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll interval 60
```

To set the interval of ping polling to the default (30 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll interval
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server ping-poll reauth-timer-refresh

Overview This command modifies the **reauth-timer-refresh** parameter for the Web-Authentication feature. The **reauth-timer-refresh** parameter specifies whether a re-authentication timer is reset and when the response from a supplicant (a client device) is received.

Use the **no** variant of this command to reset the **reauth-timer-refresh** parameter to the default setting (disabled).

Syntax

```
auth-web-server ping-poll reauth-timer-refresh
no auth-web-server ping-poll reauth-timer-refresh
```

Default The `reauth-timer-refresh` parameter is disabled by default.

Mode Global Configuration

Examples To enable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll reauth-timer-refresh
```

To disable the `reauth-timer-refresh` timer, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll
reauth-timer-refresh
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server ping-poll timeout

Overview This command modifies the ping poll **timeout** parameter for the Web-Authentication feature. The **timeout** parameter specifies the time in seconds to wait for a response to a ping packet.

Use the **no** variant of this command to reset the timeout of ping polling to the default (1 second).

Syntax

```
auth-web-server ping-poll timeout <1-30>
no auth-web-server ping-poll timeout
```

Parameter	Description
<1-30>	Seconds.

Default The default timeout for ping polling is 1 second.

Mode Global Configuration

Examples To set the timeout of ping polling to 2 seconds, use the command:

```
awplus# configure terminal
awplus(config)# auth-web-server ping-poll timeout 2
```

To set the timeout of ping polling to the default (1 second), use the command:

```
awplus# configure terminal
awplus(config)# no auth-web-server ping-poll timeout
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server port

Overview This command sets the HTTP port number for the Web-Authentication server.

Use the **no** variant of this command to reset the HTTP port number to the default (80).

Syntax

```
auth-web-server port <port-number>
no auth-web-server port
```

Parameter	Description
<port-number>	Set the local Web-Authentication server port within the TCP port number range 1 to 65535.

Default The Web-Authentication server HTTP port number is set to 80 by default.

Mode Global Configuration

Examples To set the HTTP port number `8080` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server port 8080
```

To reset to the default HTTP port number `80` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server port
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server redirect-delay-time

Overview Use this command to set the delay time in seconds before redirecting the supplicant to a specified URL when the supplicant is authorized.

Use the variant **no** to reset the delay time set previously.

Syntax

```
auth-web-server redirect-delay-time <5-60>
no auth-web-server redirect-delay-time
```

Parameter	Description
`redirect-delay-time`	Set the delay time before jumping to a specified URL after the supplicant is authorized.
<5-60>	The time in seconds.

Default The default redirect delay time is `5` seconds.

Mode Global Configuration

Examples To set the delay time to `60` seconds for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-delay-time 60
```

To reset the delay time, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-delay-time
```

Related Commands

auth-web-server blocking-mode

auth-web-server redirect-url

show auth-web-server

show running-config

auth-web-server redirect-url

Overview This command sets a URL for supplicant (client device) authentication. When a supplicant is authorized it will be automatically redirected to the specified URL. Note that if the http redirect feature is used then this command is ignored.

Use the **no** variant of this command to delete the URL string set previously.

Syntax

```
auth-web-server redirect-url <url>
no auth-web-server redirect-url
```

Parameter	Description
<url>	URL (hostname or dotted IP notation).

Default The redirect URL for the Web-Authentication server feature is not set by default (null).

Mode Global Configuration

Examples To enable and set redirect a URL string `www.alliedtelesis.com` for the Web-Authentication server, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server redirect-url
http://www.alliedtelesis.com
```

To delete a redirect URL string, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server redirect-url
```

Validation Commands show auth

show auth-web-server

show running-config

Related Commands auth-web-server http-redirect (deleted)

auth-web-server redirect-delay-time

auth-web-server session-keep

Overview This command enables the session-keep feature to jump to the original URL after being authorized by Web-Authentication.

Use the **no** variant of this command to disable the session keep feature.

Syntax
```
auth-web-server session-keep
no auth-web-server session-keep
```

Default The session-keep feature is disabled by default.

Mode Global Configuration

Usage This function doesn't ensure to keep session information in all cases. Authenticated supplicant may be redirected to unexpected page when session-keep is enabled. This issue occurred by supplicant sending HTTP packets automatically after authentication page is displayed and the URL is written.

Examples To enable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server session-keep
```

To disable the session-keep feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server session-keep
```

Validation Commands

show auth

show auth-web-server

show running-config

auth-web-server ssl

Overview This command enables HTTPS functionality for the Web-Authentication server feature.

Use the **no** variant of this command to disable HTTPS functionality for the Web-Authentication server.

Syntax

```
auth-web-server ssl
no auth-web-server ssl
```

Default HTTPS functionality for the Web-Authentication server feature is disabled by default.

Mode Global Configuration

Examples To enable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl
```

To disable HTTPS functionality for the Web-Authentication server feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl
```

Validation Commands show auth

show auth-web-server

show running-config

auth-web-server sslport (deleted)

Overview This command has been deleted in Software Version 5.4.4-2.3 and later, because it is no longer necessary to set the port number. The default port number 443 is used.

auth-web-server ssl intercept-port

Overview Use this command to register HTTPS intercept port numbers when the HTTPS server uses custom port number (not TCP port number 443).

Note that you need to use the **auth-web-server intercept-port** command to register HTTP intercept port numbers.

Use the **no** variant of this command to delete registered port number.

Syntax

```
auth-web-server ssl intercept-port <1-65535>
no auth-web-server ssl intercept-port <1-65535>
```

Parameter	Description
<1-65535>	TCP port number in the range from 1 through 65535

Default 443/TCP is registered by default.

Mode Global Configuration

Examples To register HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# auth-web-server ssl intercept-port 3128
```

To delete HTTPS port number 3128, use the commands:

```
awplus# configure terminal
awplus(config)# no auth-web-server ssl intercept-port 3128
```

Validation Commands show auth-web-server

Related Commands auth-web-server intercept-port

copy proxy-autoconfig-file

Overview Use this command to download the proxy auto configuration (PAC) file to your switch. The Web-Authentication supplicant can get the downloaded file from the system web server.

Syntax

```
copy <filename> proxy-autoconfig-file
```

Parameter	Description
<filename>	The URL of the PAC file.

Mode Privileged Exec

Example To download the PAC file to this device, use the command:

```
awplus# copy tftp://server/proxy.pac proxy-autoconfig-file
```

Related Commands

show proxy-autoconfig-file

erase proxy-autoconfig-file

copy web-auth-https-file

Overview Use this command to download the SSL server certificate for web-based authentication. The file must be in PEM (Privacy Enhanced Mail) format, and contain the private key and the server certificate.

Syntax

```
copy <filename> web-auth-https-file
```

Parameter	Description
<filename>	The URL of the server certificate file.

Mode Privileged Exec

Example To download the server certificate file `veriSign_cert.pem` from the TFTP server directory `server`, use the command:

```
awplus# copy tftp://server/veriSign_cert.pem
web-auth-https-file
```

Related Commands

auth-web-server ssl

erase web-auth-https-file

show auth-web-server

description (Authentication Profile)

Overview Use this command to add a description to an authentication profile in Authentication Profile mode.

Use the **no** variant of this command to remove the current description.

Syntax

```
description <description>
```

Parameter	Description
<description>	Text describing the selected authentication profile.

Default No description configured by default.

Mode Authentication Profile

Example To add a description to the authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# description student room setting
```

To remove a description from the authentication profile 'student', use the following commands:

```
awplus# configure terminal
awplus(config)# auth profile student
awplus(config-auth-profile)# no description
```

Related Commands auth profile (Global Configuration)

erase proxy-autoconfig-file

Overview Use this command to remove the proxy auto configuration file.

Syntax

```
erase proxy-autoconfig-file
```

Mode Privileged Exec

Example To remove the proxy auto configuration file, use the command:

```
awplus# erase proxy-autoconfig-file
```

Related Commands

show proxy-autoconfig-file

copy proxy-autoconfig-file

erase web-auth-https-file

Overview Use this command to remove the SSL server certificate for web-based authentication.

Syntax

```
erase web-auth-https-file
```

Mode Privileged Exec

Example To remove the SSL server certificate file for web-based authentication use the command:

```
awplus# erase web-auth-https-file
```

Related Commands

auth-web-server ssl

copy web-auth-https-file

show auth-web-server

platform l3-vlan-hashing-algorithm

Overview This command enables you to change the L3 VLAN hash-key-generating algorithm.

The **no** variant of this command returns the hash-key algorithm to the default of crc32l.

Syntax

```
platform l3-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
```

```
no platform l3-vlan-hashing-algorithm
```

Parameter	Description
`crc16l`	The algorithm that will apply to the lower bits of CRC-16
`crc16u`	The algorithm that will apply to the upper bits of CRC-16
`crc32l`	The algorithm that will apply to the lower bits of CRC-32
`crc32u`	The algorithm that will apply to the upper bits of CRC-32

Default The hash-key algorithm is crc32l by default.

Mode Global configuration

Usage Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN L3 table. This can happen when more than four different IP addresses produce the same hash-key.

A work-around when this situation occurs, can sometimes be applied by changing the hashing algorithm from its default of crc32l. Several different algorithms may need to be tried to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm applying to the lower bits of CRC-16, use the command:

```
awplus# configure terminal
awplus(config)# platform l3-vlan-hashing-algorithm crc16l
```

Related Commands platform mac-vlan-hashing-algorithm

show platform

platform mac-vlan-hashing-algorithm

Overview This command enables you to change the MAC VLAN hash-key-generating algorithm.

Syntax

```
platform mac-vlan-hashing-algorithm
{crc16l|crc16u|crc32l|crc32u}
```

```
no platform mac-vlan-hashing-algorithm
```

Parameter	Description
`crc16l`	The algorithm that will apply to the lower bits of CRC-16
`crc16u`	The algorithm that will apply to the upper bits of CRC-16
`crc32l`	The algorithm that will apply to the lower bits of CRC-32
`crc32u`	The algorithm that will apply to the upper bits of CRC-32

Default The hash-key algorithm is crc32l by default.

Mode Global configuration

Usage Occasionally, when using the Multiple Dynamic VLAN feature, a supplicant cannot be authenticated because a collision occurs within the VLAN MAC table. This can happen when more than four different MAC addresses produce the same hash-key.

A work-around when this situation occurs, can sometimes be applied by changing the hashing algorithm from its default of crc32l. Several different algorithms may need to be tried to rectify the problem.

You must restart the switch for this command to take effect.

Note that this command is intended for technical support staff, or advanced end users.

Example To change the hash-key generating algorithm applying to the lower bits of CRC-16, use the command:

```
awplus# configure terminal
awplus(config)# platform mac-vlan-hashing-algorithm crc16l
```

Related Commands platform l3-vlan-hashing-algorithm

show platform

show auth

Overview This command shows the configuration state of authentication.

Syntax

```
show auth [all]
```

Parameter	Description
`all`	Display all authentication information for each authenticated interface. This can be a static channel (or static aggregator), or a dynamic (or LACP) channel group, or a switch port.

Mode Privileged Exec

Example To display all authentication information, enter the command:

```
awplus# show auth all
```

Output Figure 30-1: Example output from the **show auth** command

```
awplus# show auth all
802.1X Port-Based Authentication Enabled
MAC-based Port Authentication Disabled
WEB-based Port Authentication Enabled
 RADIUS server address (auth): 150.87.17.192:1812
   Last radius message id: 4
Authentication Info for interface port1.0.1 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
```

```
twoStepAuthentication:
   configured: enabled
   actual: enabled
supplicantMac: none
Supplicant name: oha
Supplicant address: 000d.6013.5398
   authenticationMethod: WEB-based Authentication
   Two-Step Authentication:
     firstAuthentication: Pass - Method: dot1x
     secondAuthentication: Pass - Method: web
   portStatus: Authorized - currentId: 3
   abort:F fail:F start:F timeout:F success:T
   PAE: state: Authenticated - portMode: Auto
   PAE: reAuthCount: 0 - rxRespId: 0
   PAE: quietPeriod: 60 - maxReauthReq: 2
   BE: state: Idle - reqCount: 0 - idFromServer: 2
   CD: adminControlledDirections: in - operControlledDirections: in
   CD: bridgeDetected: false
   KR: rxKey: false
   KT: keyAvailable: false - keyTxEnabled: false
```

Related Commands show dot1x

show auth diagnostics

Overview This command shows authentication diagnostics, optionally for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

If no interface is specified then authentication diagnostics are shown for all interfaces.

Syntax

```
show auth diagnostics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify ports to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication diagnostics for `port1.0.6`, enter the command:

```
awplus# show auth diagnostics interface port1.0.6
```

Output Figure 30-2: Example output from the **show auth diagnostics** command

```
Authentication Diagnostics
for interface port1.0.6
     Supplicant address: 00d0.59ab.7037
         authEnterConnecting: 2
         authEaplogoffWhileConnecting: 1
         authEnterAuthenticating: 2
         authSuccessWhileAuthenticating: 1
         authTimeoutWhileAuthenticating: 1
         authFailWhileAuthenticating: 0
         authEapstartWhileAuthenticating: 0
         authEaplogoggWhileAuthenticating: 0
         authReauthsWhileAuthenticated: 0
         authEapstartWhileAuthenticated: 0
         authEaplogoffWhileAuthenticated: 0
         BackendResponses: 2
         BackendAccessChallenges: 1
         BackendOtherrequestToSupplicant: 3
         BackendAuthSuccess: 1
```

Related Commands show dot1x interface

show auth interface

Overview This command shows the status of port authentication on the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Use the optional **diagnostics** parameter to show authentication diagnostics for the specified interface. Use the optional **sessionstatistics** parameter to show authentication session statistics for the specified interface. Use the optional **statistics** parameter to show authentication diagnostics for the specified interface. Use the optional **supplicant** (client device) parameter to show the supplicant state for the specified interface.

Syntax

```
show auth interface <interface-list>
[diagnostics|sessionstatistics|statistics|supplicant [brief]]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`diagnostics`	Diagnostics.
`sessionstatistics`	Session statistics.
`statistics`	Statistics.
`supplicant`	Supplicant (client device).
`brief`	Brief summary of supplicant state.

Mode Privileged Exec

Example To display the Web based authentication status for `port1.0.6`, enter the command:

```
awplus# show auth interface port1.0.6
```

If web-based authentication is not configured, the output will be

```
% Port-Control not configured on port1.0.6
```

To display the Web based authentication status for `port1.0.1`, enter the command:

```
awplus# show auth interface port1.0.1
```

```
awplus# show auth interface port1.0.1
Authentication Info for interface port1.0.1
 portEnabled: true - portControl: Auto
 portStatus: Authorized
 reAuthenticate: disabled
 reAuthPeriod: 3600
 PAE: quietPeriod: 60 - maxReauthReq: 2 - txPeriod: 30
 BE: suppTimeout: 30 - serverTimeout: 30
 CD: adminControlledDirections: in
 KT: keyTxEnabled: false
 critical: disabled
 guestVlan: disabled
 guestVlanForwarding:
   none
 authFailVlan: disabled
 dynamicVlanCreation: disabled
 hostMode: single-host
 dot1x: enabled
   protocolVersion: 1
 authMac: disabled
 authWeb: enabled
   method: PAP
   maxAuthFail: 3
   packetForwarding:
     10.0.0.1 80/tcp
     dns
     dhcp
 twoStepAuthentication:
   configured: enabled
   actual: enabled
 supplicantMac: none
```

To display Web-Authentication diagnostics for `port1.0.6`, enter the command:

```
awplus# show auth interface port1.0.6 diagnostics
```

```
Authentication Diagnostics for interface port1.0.6

Supplicant address: 00d0.59ab.7037
authEnterConnecting: 2
authEaplogoffWhileConnecting: 1
         authEnterAuthenticating: 2
         authSuccessWhileAuthenticating: 1
         authTimeoutWhileAuthenticating: 1
         authFailWhileAuthenticating: 0
         authEapstartWhileAuthenticating: 0
         authEaplogoggWhileAuthenticating: 0
         authReauthsWhileAuthenticated: 0
         authEapstartWhileAuthenticated: 0
         authEaplogoffWhileAuthenticated: 0
         BackendResponses: 2
         BackendAccessChallenges: 1
         BackendOtherrequestToSupplicant: 3
         BackendAuthSuccess: 1
```

To display Web-Authentication session statistics for `port1.0.6`, enter the command:

```
awplus# show auth interface port1.0.6 sessionstatistics
```

```
Authentication session statistics for interface port1.0.6
     session user name: manager
         session authentication method: Remote server
         session time: 19440 secs
         session terminat cause: Not terminated yet
```

To display Web-Authentication statistics for `port1.0.6`, enter the command:

```
awplus# show auth statistics interface port1.0.6
```

To display the Web-Authenticated supplicant on interface `port1.0.6`, enter the command:

```
awplus# show auth interface port1.0.6 supplicant
```

Related Commands

show auth diagnostics

show dot1x sessionstatistics

show dot1x statistics interface

show dot1x supplicant interface

show auth sessionstatistics

Overview This command shows authentication session statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax

```
show auth sessionstatistics [interface <interface-list>]
```

Parameter	Description
`interface`	Specify ports to show.
`<interface-list>`	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display authentication statistics for `port1.0.6`, enter the command:

```
awplus# show auth sessionstatistics interface port1.0.6
```

Output Figure 30-3: Example output from the **show auth sessionstatistics** command

```
Authentication session
statistics for interface port1.0.6
     session user name: manager
         session authentication method: Remote server
         session time: 19440 secs
         session terminat cause: Not terminated yet
```

show auth statistics interface

Overview This command shows the authentication statistics for the specified interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port.

Syntax

```
show auth statistics interface <interface-list>
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.

Mode Privileged Exec

Example To display Web-Authentication statistics for `port1.0.4`, enter the command:

```
awplus# show auth statistics interface port1.0.4
```

Related Commands show dot1x interface

show auth supplicant

Overview This command shows the supplicant (client device) state when authentication is configured for the switch. Use the optional **brief** parameter to show a summary of the supplicant state.

Syntax

```
show auth supplicant [<macadd>] [brief]
```

Parameter	Description
<macadd>	Mac (hardware) address of the supplicant. Entry format is HHHH.HHHH.HHHH (hexadecimal).
brief	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display a summary of authenticated supplicant information on the device, enter the command:

```
awplus# show auth supplicant brief
```

To display authenticated supplicant information on the device, enter the command:

```
awplus# show auth supplicant
```

To display authenticated supplicant information for device with MAC address 0000.5E00.5301, enter the command:

```
awplus# show auth supplicant 0000.5E00.5301
```

Output Figure 30-4: Example output from **show auth supplicant brief**

```
awplus#show auth supplicant brief
Interface port2.0.3
  authenticationMethod: dot1x/mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x/web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0RADIUS Group Configuration

Interface   VID  Mode MAC Address    Status            IP Address      Username
=========== ==== ==== ============== ================= =============== ========
port2.0.3   1    W    001c.233e.e15a Authenticated     192.168.1.181   test
```

Figure 30-5: Example output from **show auth supplicant**

```
awplus#show auth supplicant
Interface port2.0.3
  authenticationMethod: dot1x/mac/web
  Two-Step Authentication
    firstMethod: mac
    secondMethod: dot1x/web
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 0
    webBasedAuthenticationSupplicantNum: 1
    otherAuthenticationSupplicantNum: 0

  Supplicant name: test
  Supplicant address: 0000.5E00.5301
    authenticationMethod: WEB-based Authentication
    Two-Step Authentication:
      firstAuthentication: Pass - Method: mac
      secondAuthentication: Pass - Method: web
    portStatus: Authorized - currentId: 1
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 0
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    RADIUS server group (auth): radius
    RADIUS server (auth): 192.168.1.40
```

Figure 30-6: Example output from **show auth supplicant 0000.5E00.5301**

```
awplus#show auth supplicant 0000.5E00.5301
Interface port2.0.3
  Supplicant name: test
  Supplicant address: 0000.5E00.5301
    authenticationMethod: WEB-based Authentication
    Two-Step Authentication:
      firstAuthentication: Pass - Method: mac
      secondAuthentication: Pass - Method: web
    portStatus: Authorized - currentId: 1
    abort:F fail:F start:F timeout:F success:T
    PAE: state: Authenticated - portMode: Auto
    PAE: reAuthCount: 0 - rxRespId: 0
    PAE: quietPeriod: 60 - maxReauthReq: 2
    BE: state: Idle - reqCount: 0 - idFromServer: 0
    CD: adminControlledDirections: in - operControlledDirections: in
    CD: bridgeDetected: false
    KR: rxKey: false
    KT: keyAvailable: false - keyTxEnabled: false
    RADIUS server group (auth): radius
    RADIUS server (auth): 192.168.1.40
```

Related Commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa authentication auth-mac

aaa authentication auth-web

aaa authentication dot1x

show auth supplicant interface

Overview This command shows the supplicant (client device) state for the authentication mode set for the interface, which may be a static channel (or static aggregator) or a dynamic (or LACP) channel group or a switch port. Use the optional **brief** parameter to show a summary of the supplicant state.

Syntax

```
show auth-web supplicant interface <interface-list> [brief]
```

Parameter	Description
<interface-list>	The interfaces or ports to configure. An interface-list can be: • an interface (e.g. `vlan2`), a switch port (e.g. `port1.0.6`), a static channel group (e.g. `sa2`) or a dynamic (LACP) channel group (e.g. `po2`) • a continuous range of interfaces, ports, static channel groups or dynamic (LACP) channel groups separated by a hyphen; e.g. `vlan2-8`, or `port1.0.1-1.0.4`, or `sa1-2`, or `po1-2` • a comma-separated list of the above; e.g. `port1.0.1,port1.0.4-1.0.6`. Do not mix interface types in a list The specified interfaces must exist.
`brief`	Brief summary of the supplicant state.

Mode Privileged Exec

Examples To display the authenticated supplicant on the interface `port1.0.3`, enter the command:

```
awplus# show auth supplicant interface port1.0.3
```

To display brief summary output for the authenticated supplicant, enter the command:

```
awplus# show auth supplicant brief
```

show auth two-step supplicant brief

Overview This command displays the supplicant state of the two-step authentication feature on the interface.

Syntax

```
show auth two-step supplicant [interface <ifrange>] brief
```

Parameter	Description
`interface`	The interface selected for display.
<ifrange>	The interface types which can be specified as *<ifrange>* • Switch port (e.g. port1.0.6) • Static channel group (e.g. sa3) • Dynamic (LACP) channel group (e.g. po4)

Mode Privileged Exec

Usage Do not mix interface types in a list. The specified interfaces must exist.

Example To display the supplicant state of the two-step authentication feature, enter the command:

```
awplus# show two-step supplicant interface port1.0.6 brief
```

Output Figure 30-7: Example output from **show auth two-step supplicant brief**

```
interface port1.0.6

  authenticationMethod: dot1x/mac

  Two-Step Authentication:
    firstMethod:mac
    secondMethod:dot1x
  totalSupplicantNum: 1
  authorizedSupplicantNum: 1
    macBasedAuthenticationSupplicantNum: 0
    dot1xAuthenticationSupplicantNum: 1
    webBasedAuthenticationSupplicantNum: 0
    otherAuthenticationSupplicantNum: 0

Interface  VID Mode  MAC Address       Status          FirstStep     SecondStep
========== === ====  ===========       ======          =========     ==========
port1.0.6  1   D     000b..db67.00f7   Authenticated   Pass          Pass
```

Related Commands auth two-step enable

show auth-web-server

Overview This command shows the Web-Authentication server configuration and status on the switch.

Syntax

```
show auth-web-server
```

Mode Privileged Exec

Example To display Web-Authentication server configuration and status, enter the command:

```
awplus# show auth-web-server
```

Output Figure 30-8: Example output from the **show auth-web-server** command

```
Web authentication server
     Server status: enabled
     Server mode: none
     Server address: 192.168.1.1/24
       DHCP server enabled
       DHCP lease time: 20
       DHCP WPAD Option URL: http://192.168.1.1/proxy.pac
     HTTP Port No: 80
     Security: disabled
     Certification: default
     SSL Port No: 443
     Redirect URL: --
     Redirect Delay Time: 5
     HTTP Redirect: enabled
     Session keep: disabled
     PingPolling: disabled
     PingInterval: 30
     Timeout: 1
     FailCount: 5
     ReauthTimerReFresh: disabled
```

Related Commands

auth-web-server gateway (deleted)

auth-web-server http-redirect (deleted)

auth-web-server ipaddress

auth-web-server port

auth-web-server redirect-delay-time

auth-web-server redirect-url

auth-web-server session-keep

auth-web-server ssl

auth-web-server sslport (deleted)

show auth-web-server page

Overview This command displays the web-authentication page configuration and status.

Syntax

```
show auth-web-server page
```

Mode Privileged Exec

Examples To show the web-authentication page information, use the command:

```
awplus# show auth-web-server page
```

Figure 30-9: Example output from the **show auth-web-server page** command

```
awplus#show auth-web-server page
Web authentication page
  Logo: auto
  Title: default
  Sub-Title: Web Authentication
  Welcome message: Your welcome message
  Success message: Your success message
```

Related Commands

auth-web forward

auth-web-server page logo

auth-web-server page sub-title

auth-web-server page success-message

auth-web-server page title

auth-web-server page welcome-message

show proxy-autoconfig-file

Overview This command displays the contents of the proxy auto configuration (PAC) file.

Syntax

```
show proxy-autoconfig-file
```

Mode Privileged Exec

Example To display the contents of the proxy auto configuration (PAC) file, enter the command:

```
awplus# show auth proxy-autoconfig-file
```

Output Figure 30-10: Example output from the **show proxy-autoconfig**-file

```
function FindProxyForURL(url,host)
{
 if (isPlainHostName(host) ||
     isInNet(host, "192.168.1.0","255.255.255.0")) {
   return "DIRECT";
}
 else {
   return "PROXY 192.168.110.1:8080";
 }
}
```

Related Commands

copy proxy-autoconfig-file

erase proxy-autoconfig-file

31 AAA Commands

Introduction

Overview This chapter provides an alphabetical reference for AAA commands for Authentication, Authorization and Accounting. For more information, see the AAA Feature Overview and Configuration Guide.

Command List

aaa accounting auth-mac

Overview This command configures an accounting method list for MAC-based authentication. An accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. Use this command to configure either the default method list, which is automatically applied to interfaces with MAC-based authentication enabled, or a named method list, which can be applied to an interface with the auth-mac accounting command.

Use the **no** variant of this command to disable either the default or a named accounting method list for MAC-based authentication. Once all method lists are disabled, AAA accounting for MAC-based authentication is disabled globally.

Syntax
```
aaa accounting auth-mac {default|<list-name>}
{start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting auth-mac {default|<list-name>}
```

Parameter	Description
`default`	Configure the default accounting method list
`<list-name>`	Configure a named accounting method list
`start-stop`	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
`stop-only`	Only sends a stop accounting message at the end of the session.
`none`	No accounting record sent.
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for MAC-based Authentication is disabled by default

Mode Global Configuration

Usage This command can be used to configure either the default accounting method list or a named accounting method list:

- **default**: the default accounting method list which is automatically applied to all interfaces with MAC-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the auth-mac accounting command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command

- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command

The accounting event to send to the RADIUS server is configured with the following options:

- **start-stop**: sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only**: sends a **stop** accounting message at the end of a session.
- **none**: disables accounting.

Examples

To enable the default RADIUS accounting for MAC-based authentication, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac default start-stop
group radius
```

To disable RADIUS accounting for MAC-based Authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac default
```

To enable a named RADIUS accounting method list 'vlan10_acct' for MAC-based authentication, with the RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-mac vlan10_acct start-stop
group rad_group_vlan10
```

To disable a named RADIUS accounting method list 'vlan10_acct' for MAC-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-mac vlan10_acct
```

Related Commands

aaa authentication auth-mac

aaa group server

auth-mac accounting

auth-mac enable

radius-server host

show aaa server group

aaa accounting auth-web

Overview This command configures an accounting method list for Web-based authentication. An accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. Use this command to configure either the default method list, which is automatically applied to interfaces with Web-based authentication enabled, or a named method list, which can be applied to an interface with the auth-web accounting command.

Use the **no** variant of this command to disable either the default or a named accounting method list for Web-based authentication. Once all method lists are disabled, AAA accounting for Web-based authentication is disabled globally.

Syntax

```
aaa accounting auth-web {default|<list-name>}
{start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting auth-web {default|<list-name>}
```

Parameter	Description
`default`	Configure the default accounting method list
`<list-name>`	Configure a named accounting method list
`start-stop`	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
`stop-only`	Only sends a stop accounting message at the end of the session.
`none`	No accounting record sent.
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for Web-based authentication is disabled by default.

Mode Global Configuration

Usage This command can be used to configure either the default accounting method list or a named accounting method list:

- **default**: the default accounting method list which is automatically applied to all interfaces with Web-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the auth-web accounting command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command

- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command

Configure the accounting event to be sent to the RADIUS server with the following options:

- **start-stop**: sends a start accounting message at the beginning of a session and a stop accounting message at the end of the session.
- **stop-only**: sends a stop accounting message at the end of a session.
- **none**: disables accounting.

Examples To enable the default RADIUS accounting method for Web-based authentication, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web default start-stop
group radius
```

To disable the default RADIUS accounting method for Web-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web default
```

To enable a named RADIUS accounting method list 'vlan10_acct' for Web-based authentication, with the RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting auth-web vlan10_acct start-stop
group rad_group_vlan10
```

To disable a named RADIUS accounting method list 'vlan10_acct' for Web-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting auth-web vlan10_acct
```

Related Commands

aaa authentication auth-web

aaa group server

auth-web accounting

auth-web enable

radius-server host

show aaa server group

aaa accounting commands

Overview This command configures and enables TACACS+ accounting on commands entered at a specified privilege level. Once enabled for a privilege level, accounting messages for commands entered at that privilege level will be sent to a TACACS+ server.

In order to account for all commands entered on a device, configure command accounting for each privilege level separately.

The command accounting message includes, the command as entered, the date and time the command finished executing, and the user-name of the user who executed the command.

Use the **no** variant of this command to disable command accounting for a specified privilege level.

Syntax

```
aaa accounting commands <1-15> default stop-only group tacacs+
no aaa accounting commands <1-15> default
```

Parameter	Description
<1-15>	The privilege level being configured, in the range 1 to 15.
`default`	Use the default method list, this means the command is applied globally to all user exec sessions.
`stop-only`	Send accounting message when the commands have stopped executing.
`group`	Specify the server group where accounting messages are sent. Only the tacacs+ group is available for this command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.

Default TACACS+ command accounting is disabled by default.

Mode Global Configuration

Usage This command only supports a **default** method list, this means that it is applied to every console and vty line.

The **stop-only** parameter indicates that the command accounting messages are sent to the TACACS+ server when the commands have stopped executing.

The **group tacacs+** parameters signifies that the command accounting messages are sent to the TACACS+ servers configured by the tacacs-server host command.

Note that up to four TACACS+ servers can be configured for accounting. The servers are checked for reachability in the order they are configured with only the first reachable server being used. If no server is found, the accounting message is dropped.

Command accounting cannot coexist with triggers. An error message is displayed if you attempt to enable command accounting while a trigger is configured. Likewise, an error message is displayed if you attempt to configure a trigger while command accounting is configured.

Examples

To configure command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting commands 1 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 7 default stop-only
group tacacs+
awplus(config)# aaa accounting commands 15 default stop-only
group tacacs+
```

To disable command accounting for privilege levels 1, 7, and 15, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting commands 1 default
awplus(config)# no aaa accounting commands 7 default
awplus(config)# no aaa accounting commands 15 default
```

Related Commands

aaa authentication login

aaa accounting login

accounting login

tacacs-server host

aaa accounting dot1x

Overview This command configures an accounting method list for IEEE 802.1X-based authentication. An accounting method list specifies what type of accounting messages are sent and which RADIUS servers the accounting messages are sent to. Use this command to configure either the default method list, which is automatically applied to interfaces with IEEE 802.1X-based authentication enabled, or a named method list, which can be applied to an interface with the dot1x accounting command.

Use the **no** variant of this command to disable either the default or a named accounting method list for 802.1X-based authentication. Once all method lists are disabled, AAA accounting for 802.1x-based authentication is disabled globally.

Syntax

```
aaa accounting dot1x {default|<list-name>}
{start-stop|stop-only|none} group {<group-name>|radius}
no aaa accounting dot1x {default|<list-name>}
```

Parameter	Description
`default`	Configure the default accounting method list
`<list-name>`	Configure a named accounting method list
`start-stop`	Sends a start accounting message at the beginning of the session and a stop accounting message at the end of the session.
`stop-only`	Only sends a stop accounting message at the end of the session.
`none`	No accounting record sent.
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default RADIUS accounting for 802.1X-based authentication is disabled by default (there is no default server set by default).

Mode Global Configuration

Usage This command can be used to configure either the default accounting method list or a named accounting method list:

- **default**: the default accounting method list which is automatically applied to all interfaces with 802.1X-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the dot1x accounting command.

There are two ways to define servers where RADIUS accounting messages will be sent:

- **group radius**: use all RADIUS servers configured by radius-server host command.
- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command.

The accounting event to send to the RADIUS server is configured by the following options:

- **start-stop**: sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only**: sends a **stop** accounting message at the end of a session.
- **none**: disables accounting.

Examples

To enable RADIUS accounting for 802.1X-based authentication, and use all available RADIUS Servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting dot1x default start-stop group radius
```

To disable RADIUS accounting for 802.1X-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting dot1x default
```

To enable a named RADIUS accounting method list 'vlan10_acct' for 802.1X-based authentication, with the RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa accounting dot1x vlan10_acct start-stop group rad_group_vlan10
```

To disable a named RADIUS accounting method list 'vlan10_acct' for 802.1X-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting dot1x vlan10_acct
```

Related Commands

aaa accounting update

aaa authentication dot1x

aaa group server

dot1x accounting

dot1x port-control

radius-server host

show aaa server group

aaa accounting login

Overview This command configures RADIUS and TACACS+ accounting for login shell sessions. The specified method list name can be used by the **accounting login** command in the Line Configuration mode. If the **default** parameter is specified, then this creates a default method list that is applied to every console and vty line, unless another accounting method list is applied on that line.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to remove an accounting method list for login shell sessions configured by an **aaa accounting login** command. If the method list being deleted is already applied to a console or vty line, accounting on that line will be disabled. If the default method list name is removed by this command, it will disable accounting on every line that has the default accounting configuration.

Syntax

```
aaa accounting login
{default|<list-name>}{start-stop|stop-only|none} {group
{radius|tacacs+|<group-name>}}
```

```
no aaa accounting login {default|<list-name>}
```

Parameter	Description
`default`	Default accounting method list.
`<list-name>`	Named accounting method list.
`start-stop`	Start and stop records to be sent.
`stop-only`	Stop records to be sent.
`none`	No accounting record to be sent.
`group`	Specify the servers or server group where accounting packets are sent.
`radius`	Use all RADIUS servers configured by the radius-server host command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.
`<group-name>`	Use the specified RADIUS server group, as configured by the aaa group server command.

Default Accounting for login shell sessions is disabled by default.

Mode Global Configuration

Usage This command enables you to define a named accounting method list. The items that you define in the accounting options are:

- the types of accounting packets that will be sent
- the set of servers to which the accounting packets will be sent

You can define a default method list with the name **default** and any number of other named method lists. The name of any method list that you define can then be used as the *<list-name>* parameter in the accounting login command.

If the method list name already exists, the command will replace the existing configuration with the new one.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius** : use all RADIUS servers configured by radius-server host command
- **group** *<group-name>* : use the specified RADIUS server group configured with the aaa group server command

There is one way to define servers where TACACS+ accounting messages are sent:

- **group tacacs+** : use all TACACS+ servers configured by tacacs-server host command

The accounting event to send to the RADIUS or TACACS+ server is configured with the following options:

- **start-stop** : sends a **start** accounting message at the beginning of a session and a **stop** accounting message at the end of the session.
- **stop-only** : sends a **stop** accounting message at the end of a session.
- **none** : disables accounting.

Examples To configure RADIUS accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group radius
```

To configure TACACS+ accounting for login shell sessions, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting login default start-stop group tacacs+
```

To reset the configuration of the default accounting list, use the following commands:

```
awplus# configure terminal
awplus(config)#  no aaa accounting login default
```

Related Commands

aaa accounting commands

aaa authentication login

aaa accounting login

aaa accounting update

accounting login

radius-server host

tacacs-server host

aaa accounting update

Overview This command enables periodic accounting reporting to either the RADIUS or TACACS+ accounting server(s) wherever login accounting has been configured.

Note that unlimited RADIUS servers and up to four TACACS+ servers can be configured and consulted for accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, i.e. is unreachable.

Use the **no** variant of this command to disable periodic accounting reporting to the accounting server(s).

Syntax

```
aaa accounting update [periodic <1-65535>]
no aaa accounting update
```

Parameter	Description
`periodic`	Send accounting records periodically.
<1-65535>	The interval to send accounting updates (in minutes). The default is 30 minutes.

Default Periodic accounting update is disabled by default.

Mode Global Configuration

Usage Use this command to enable the device to send periodic AAA login accounting reports to the accounting server. When periodic accounting report is enabled, interim accounting records are sent according to the interval specified by the **periodic** parameter. The accounting updates are start messages.

If the **no** variant of this command is used to disable periodic accounting reporting, any interval specified by the **periodic** parameter is reset to the default of 30 minutes when accounting reporting is reenabled, unless this interval is specified.

Examples To configure the switch to send period accounting updates every 30 minutes, the default period, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update
```

To configure the switch to send period accounting updates every 10 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa accounting update periodic 10
```

To disable periodic accounting update wherever accounting has been configured, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa accounting update
```

Related Commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting login

aaa authentication auth-mac

Overview This command enables MAC-based authentication globally and allows you to enable either the default authentication method list (in this case, a list of RADIUS servers), which is automatically applied to every interface running MAC-based authentication, or a user named authentication method list, which is applied to an interface with the auth-mac authentication command.

Use the **no** variant of this command to disable either the default or a named method list for MAC-based authentication. Once all method lists are disabled MAC-based authentication is disabled globally.

Syntax

```
aaa authentication auth-mac {default|<list-name>} group
{<group-name>|radius}
```

```
no aaa authentication auth-mac {default|<list-name>}
```

Parameter	Description
`default`	Configure the default authentication method list
`<list-name>`	Configure a named authentication method list
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default MAC-based Port Authentication is disabled by default.

Mode Global Configuration

Usage This command can be used to configure either the default authentication method list or a named authentication method list:

- **default**: the default authentication method list which is automatically applied to all interfaces with Web-based authentication enabled.
- **<***list-name***>**: a user named list which can be applied to an interface using the auth-web authentication command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group** <*group-name*>: use the specified RADIUS server group configured with the aaa group server command

All configured RADIUS Servers are automatically members of the server group **radius**. If a server is added to a named group <*group-name*>, it also remains a member of the group **radius**.

Examples

To enable MAC-based authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac default group radius
```

To disable MAC-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac default
```

To enable MAC-based authentication for named list 'vlan10_auth', with RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-mac vlan10_auth group rad_group_vlan10
```

To disable MAC-based authentication for named list 'vlan10_auth', use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-mac vlan10_acct
```

Related Commands

aaa accounting auth-mac

aaa group server

auth-mac authentication

auth-mac enable

radius-server host

show aaa server group

aaa authentication auth-web

Overview This command enables Web-based authentication globally and allows you to enable either the default authentication method list (in this case, a list of RADIUS servers), which is automatically applied to every interface running Web-based authentication, or a user named authentication method list, which is applied to an interface with the auth-web authentication command.

Use the **no** variant of this command to disable either the default or a named method list for Web-based authentication. Once all method lists are disabled Web-based authentication is disabled globally.

Syntax

```
aaa authentication auth-web {default|<list-name>} group
{<group-name>|radius}
```

```
no aaa authentication auth-web {default|<list-name>}
```

Parameter	Description
`default`	Configure the default authentication method list
`<list-name>`	Configure a named authentication method list
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default Web-based authentication is disabled by default.

Mode Global Configuration

Usage This command can be used to configure either the default authentication method list or a named authentication method list:

- **default**: the default authentication method list which is automatically applied to all interfaces with Web-based authentication enabled.
- **<***list-name***>**: a user named list which can be applied to an interface using the auth-web authentication command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group <***group-name***>**: use the specified RADIUS server group configured with the aaa group server command

Note that you need to configure an IPv4 address for the VLAN interface on which Web authentication is running.

Examples

To enable Web-based authentication globally for all RADIUS servers, and use all available RADIUS servers, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web default group radius
```

To disable Web-based authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication auth-web default
```

To enable Web-based authentication for named list 'vlan10_auth', with RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication auth-web vlan10_auth group rad_group_vlan10
```

To disable Web-based authentication for named list 'vlan10_auth', use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication vlan10_acct
```

Related Commands

aaa accounting auth-web

aaa group server

auth-web authentication

auth-web enable

radius-server host

aaa authentication dot1x

Overview This command enables IEEE 802.1X-based authentication globally and allows you to enable either the default authentication method list (in this case, a list of RADIUS servers), which is automatically applied to every interface running IEEE 802.1X-based authentication, or a user named authentication method list, which is applied to an interface with the dot1x authentication command.

Use the **no** variant of this command to disable either the default or a named method list for 802.1X-based authentication. Once all method lists are disabled 802.1x-based authentication is disabled globally.

Syntax

```
aaa authentication dot1x {default|<list-name>} group
{<group-name>|radius}
```

```
no aaa authentication dot1x {default|<list-name>}
```

Parameter	Description
`default`	Configure the default authentication method list
`<list-name>`	Configure a named authentication method list
`group`	Use a server group
`<group-name>`	Server group name.
`radius`	Use all RADIUS servers.

Default 802.1X-based Port Authentication is disabled by default.

Mode Global Configuration

Usage This command can be used to configure either the default authentication method list or a named authentication method list:

- **default**: the default authentication method list which is automatically applied to all interfaces with 802.1X-based authentication enabled.
- *<list-name>*: a user named list which can be applied to an interface using the aaa authentication dot1x command.

There are two ways to define servers where RADIUS accounting messages are sent:

- **group radius**: use all RADIUS servers configured by radius-server host command
- **group** *<group-name>*: use the specified RADIUS server group configured with the aaa group server command

Examples To enable 802.1X-based authentication globally with all RADIUS servers, and use all available RADIUS servers, use the command:

```
awplus# configure terminal
```

```
awplus(config)# aaa authentication dot1x default group radius
```

To disable 802.1X-based authentication, use the command:

```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x default
```

To enable 802.1X-based authentication for named list 'vlan10_auth', with RADIUS server group 'rad_group_vlan10, use the commands:

```
awplus# configure terminal
awplus(config)# aaa authentication dot1x vlan10_auth group
rad_group_vlan10
```

To disable 802.1X-based authentication for named list 'vlan10_auth use the commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication dot1x vlan10_acct
```

Related Commands

aaa accounting dot1x

aaa group server

dot1x authentication

dot1x port-control

radius-server host

show aaa server group

aaa authentication enable default group tacacs+

Overview This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated against the TACACS+ server.

Use the **no** variant of this command to disable privilege level authentication.

Syntax

```
aaa authentication enable default group tacacs+ [local] [none]
no aaa authentication enable default
```

Parameter	Description
`local`	Use the locally configured enable password (**enable password** command) for authentication.
`none`	No authentication.

Default Local privilege level authentication is enabled by default (aaa authentication enable default local command).

Mode Global Configuration

Usage A user is configured on a TACACS+ server with a maximum privilege level. When they enter the enable (Privileged Exec mode) command they are prompted for an enable password which is authenticated against the TACACS+ server. If the password is correct and the specified privilege level is equal to or less than the users maximum privilege level, then they are granted access to that level. If the user attempts to access a privilege level that is higher than their maximum configured privilege level, then the authentication session will fail and they will remain at their current privilege level.

NOTE: *If both **local** and **none** are specified, you must always specify **local** first.*

If the TACACS+ server goes offline, or is not reachable during enable password authentication, and command level authentication is configured as:

- **aaa authentication enable default group tacacs+**

  then the user is never granted access to Privileged Exec mode.

- **aaa authentication enable default group tacacs+ local**

  then the user is authenticated using the locally configured enable password, which if entered correctly grants the user access to Privileged Exec mode. If no enable password is locally configured (**enable password** command), then the enable authentication will fail until the TACACS+ server becomes available again.

- **aaa authentication enable default group tacacs+ none**

  then the user is granted access to Privileged Exec mode with no authentication. This is true even if a locally configured enable password is configured.

- **aaa authentication enable default group tacacs+ local none**

  then the user is authenticated using the locally configured enable password. If no enable password is locally configured, then the enable authentication will grant access to Privileged Exec mode with no authentication.

If the password for the user is not successfully authenticated by the server, then the user is again prompted for an enable password when they enter **enable** via the CLI.

Examples

To enable a privilege level authentication method that will not allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
```

To enable a privilege level authentication method that will allow the user to access Privileged Exec mode if the TACACS+ server goes offline, or is not reachable during enable password authentication, and a locally configured enable password is configured, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default group tacacs+
local
```

To disable privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

Related Commands

aaa authentication login

aaa authentication enable default local

enable (Privileged Exec mode)

enable password

enable secret

tacacs-server host

aaa authentication enable default local

Overview This command enables AAA authentication to determine the privilege level a user can access for passwords authenticated locally.

Syntax

```
aaa authentication enable default local
```

Default Local privilege level authentication is enabled by default.

Mode Global Configuration

Usage The privilege level configured for a particular user in the local user database is the privilege threshold above which the user is prompted for an enable (Privileged Exec mode) command.

Examples To enable local privilege level authentication command, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication enable default local
```

To disable privilege level authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication enable default
```

Related Commands

aaa authentication enable default group tacacs+

aaa authentication login

enable (Privileged Exec mode)

enable password

enable secret

tacacs-server host

aaa authentication login

Overview Use this command to create an ordered list of methods to use to authenticate user login, or to replace an existing method list with the same name. Specify one or more of the options **local** or **group**, in the order you want them to be applied. If the **default** method list name is specified, it is applied to every console and VTY line immediately unless another method list is applied to that line by the login authentication command. To apply a non-default method list, you must also use the login authentication command.

Use the **no** variant of this command to remove an authentication method list for user login. The specified method list name is deleted from the configuration. If the method list name has been applied to any console or VTY line, user login authentication on that line will fail.

Note that the **no aaa authentication login default** command does not remove the default method list. This will return the default method list to its default state (**local** is the default).

Syntax

```
aaa authentication login {default|<list-name>} {[local] [group
{radius|tacacs+|<group-name>}]}
no aaa authentication login {default|<list-name>}
```

Parameter	Description
`default`	Set the default authentication server for user login.
`<list-name>`	Name of authentication server.
`local`	Use the local username database.
`group`	Use server group.
`radius`	Use all RADIUS servers configured by the radius-server host command.
`tacacs+`	Use all TACACS+ servers configured by the tacacs-server host command.
`<group-name>`	Use the specified RADIUS server group, as configured by the aaa group server command.

Default If the default server is not configured using this command, user login authentication uses the local user database only.

If the **default** method list name is specified, it is applied to every console and VTY line immediately unless a named method list server is applied to that line by the **loginauthentication** command.

local is the default state for the default method list unless a named method list is applied to that line by the **login authentication** command. Reset to the default method list using the **no aaa authentication login default** command.

Mode Global Configuration

Usage

When a user attempts to log in, the switch sends an authentication request to the first authentication server in the method list. If the first server in the list is reachable and it contains a username and password matching the authentication request, the user is authenticated and the login succeeds. If the authentication server denies the authentication request because of an incorrect username or password, the user login fails. If the first server in the method list is unreachable, the switch sends the request to the next server in the list, and so on.

For example, if the method list specifies **group tacacs+ local**, and a user attempts to log in with a password that does not match a user entry in the first TACACS+ server, if this TACACS+ server denies the authentication request, then the switch does not try any other TACACS+ servers not the local user database; the user login fails.

Examples

To configure the default authentication method list for user login to first use all available RADIUS servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login default group radius
local
```

To configure a user login authentication method list called **USERS** to first use the RADIUS server group `RAD_GROUP1` for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group RAD_GROUP1
local
```

To configure a user login authentication method list called USERS to first use the TACACS+ servers for user login authentication, and then use the local user database, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa authentication login USERS group tacacs+
local
```

To return to the default method list (**local** is the default server), use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login default
```

To delete an existing authentication method list USERS created for user login authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# no aaa authentication login USERS
```

Related Commands

aaa accounting commands

aaa authentication enable default group tacacs+

login authentication

aaa group server

Overview This command configures a RADIUS server group. A server group can be used to specify a subset of RADIUS servers in **aaa** commands. The group name **radius** is predefined, which includes all RADIUS servers configured by the **radius-server host** command.

RADIUS servers are added to a server group using the **server** command. Each RADIUS server should be configured using the **radius-server host** command.

Use the **no** variant of this command to remove an existing RADIUS server group.

Syntax

```
aaa group server radius <group-name>
no aaa group server radius <group-name>
```

Parameter	Description
<group-name>	Server group name.

Mode Global Configuration

Usage Use this command to create an AAA group of RADIUS servers, and to enter Server Group Configuration mode, in which you can add servers to the group. Use a server group to specify a subset of RADIUS servers in AAA commands. Each RADIUS server must be configured by the **radius-server host** command. To add RADIUS servers to a server group, use the **server** command.

Examples To create a RADIUS server group named `GROUP1` with hosts `192.168.1.1`, `192.168.2.1` and `192.168.3.1`, use the commands:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.2.1 auth-port 1812 acct-port 1813
awplus(config-sg)# server 192.168.3.1 auth-port 1812 acct-port 1813
```

To remove a RADIUS server group named `GROUP1` from the configuration, use the command:

```
awplus(config)# no aaa group server radius GROUP1
```

Related Commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting login

aaa authentication auth-mac

aaa authentication auth-web

aaa authentication dot1x

aaa authentication login

radius-server host

server (Server Group)

show radius server group

aaa local authentication attempts lockout-time

Overview This command configures the duration of the user lockout period.

Use the **no** variant of this command to restore the duration of the user lockout period to its default of 300 seconds (5 minutes).

Syntax

```
aaa local authentication attempts lockout-time <lockout-tiime>
no aaa local authentication attempts lockout-time
```

Parameter	Description
<lockout-time>	<0-10000>. Time in seconds to lockout the user.

Mode Global Configuration

Default The default for the lockout-time is 300 seconds (5 minutes).

Usage While locked out all attempts to login with the locked account will fail. The lockout can be manually cleared by another privileged account using the clear aaa local user lockout command.

Examples To configure the lockout period to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts lockout-time
600
```

To restore the default lockout period of 5 minutes (300 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts
lockout-time
```

Related Commands aaa local authentication attempts max-fail

aaa local authentication attempts max-fail

Overview This command configures the maximum number of failed login attempts before a user account is locked out. Every time a login attempt fails the failed login counter is incremented.

Use the **no** variant of this command to restore the maximum number of failed login attempts to the default setting (five failed login attempts).

Syntax

```
aaa local authentication attempts max-fail <failed-logins>
no aaa local authentication attempts max-fail
```

Parameter	Description
<failed-logins>	<1-32>. Number of login failures allowed before locking out a user.

Mode Global Configuration

Default The default for the maximum number of failed login attempts is five failed login attempts.

Usage When the failed login counter reaches the limit configured by this command that user account is locked out for a specified duration configured by the aaa local authentication attempts lockout-time command.

When a successful login occurs the failed login counter is reset to 0. When a user account is locked out all attempts to login using that user account will fail.

Examples To configure the number of login failures that will lock out a user account to two login attempts, use the commands:

```
awplus# configure terminal
awplus(config)# aaa local authentication attempts max-fail 2
```

To restore the number of login failures that will lock out a user account to the default number of login attempts (five login attempts), use the commands:

```
awplus# configure terminal
awplus(config)# no aaa local authentication attempts max-fail
```

Related Commands aaa local authentication attempts lockout-time

clear aaa local user lockout

aaa login fail-delay

Overview Use this command to configure the minimum time period between failed login attempts. This setting applies to login attempts via the console, SSH and Telnet.

Use the **no** variant of this command to reset the minimum time period to its default value.

Syntax

```
aaa login fail-delay [<1-10>]
no aaa login fail-delay [<1-10>]
```

Parameter	Description
<1-10>	The minimum number of seconds required between login attempts

Default 1 second

Mode Global configuration

Example To apply a delay of at least 5 seconds between login attempts, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa login fail-delay 5
```

Related Commands aaa authentication login

accounting login

Overview This command applies a login accounting method list to console or VTY lines for user login. When login accounting is enabled using this command, logging events generate an accounting record to the accounting server.

The accounting method list must be configured first using this command. If an accounting method list is specified that has not been created by this command then accounting will be disabled on the specified lines.

The **no** variant of this command resets AAA Accounting applied to console or VTY lines for local or remote login. **default** login accounting is applied after issuing the **no accounting login** command. Accounting is disabled with **default**.

Syntax

```
accounting login {default|<list-name>}
no accounting login
```

Parameter	Description
`default`	Default accounting method list.
<list-name>	Named accounting method list.

Default By default login accounting is disabled in the **default** accounting server. No accounting will be performed until accounting is enabled using this command.

Mode Line Configuration

Examples To apply the accounting server `USERS` to all VTY lines, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# accounting login USERS
```

Related Commands aaa accounting commands

aaa accounting login

clear aaa local user lockout

Overview Use this command to clear the lockout on a specific user account or all user accounts.

Syntax

```
clear aaa local user lockout {username <username>|all}
```

Parameter	Description
`username`	Clear lockout for the specified user.
`<username>`	Specifies the user account.
`all`	Clear lockout for all user accounts.

Mode Privileged Exec

Examples To unlock the user account '`bob`' use the following command:

```
awplus# clear aaa local user lockout username bob
```

To unlock all user accounts use the following command:

```
awplus# clear aaa local user lockout all
```

Related Commands aaa local authentication attempts lockout-time

debug aaa

Overview This command enables AAA debugging.

Use the **no** variant of this command to disable AAA debugging.

Syntax

```
debug aaa [accounting|all|authentication|authorization]
no debug aaa [accounting|all|authentication|authorization]
```

Parameter	Description
`accounting`	Accounting debugging.
`all`	All debugging options are enabled.
`authentication`	Authentication debugging.
`authorization`	Authorization debugging.

Default AAA debugging is disabled by default.

Mode Privileged Exec

Examples To enable authentication debugging for AAA, use the command:

```
awplus# debug aaa authentication
```

To disable authentication debugging for AAA, use the command:

```
awplus# no debug aaa authentication
```

Related Commands show debugging aaa

undebug aaa

login authentication

Overview

Use this command to apply an AAA server for authenticating user login attempts from a console or remote logins on these console or VTY lines. The authentication method list must be specified by the **aaa authentication login** command. If the method list has not been configured by the **aaa authentication login** command, login authentication will fail on these lines.

Use the **no** variant of this command to reset AAA Authentication configuration to use the default method list for login authentication on these console or VTY lines.

Command Syntax

```
login authentication {default|<list-name>}
no login authentication
```

Parameter	Description
`default`	The default authentication method list. If the default method list has not been configured by the aaa authentication login command, the local user database is used for user login authentication.
<list-name>	Named authentication server.

Default

The default login authentication method list, as specified by the aaa authentication login command, is used to authenticate user login. If this has not been specified, the default is to use the local user database.

Mode

Line Configuration

Examples

To reset user authentication configuration on all VTY lines, use the following commands:

```
awplus# configure terminal
awplus(config)# line vty 0 32
awplus(config-line)# no login authentication
```

Related Commands

aaa authentication login

line

show aaa local user locked

Overview This command displays the current number of failed attempts, last failure time and location against each user account attempting to log into the device.

Note that once the lockout count has been manually cleared by another privileged account using the clear aaa local user lockout command or a locked account successfully logs into the system after waiting for the lockout time, this command will display nothing for that particular account.

Syntax

```
show aaa local user locked
```

Mode User Exec and Privileged Exec

Example To display the current failed attempts for local users, use the command:

```
awplus# show aaa local user locked
```

Output Figure 31-1: Example output from the **show aaa local user locked** command

```
awplus# show aaa local user locked
Login           Failures Latest failure     From
bob                  3    05/23/14 16:21:37  ttyS0
manager              5    05/23/14 16:31:44  192.168.1.200
```

Related Commands

aaa local authentication attempts lockout-time

aaa local authentication attempts max-fail

clear aaa local user lockout

show aaa server group

Overview Use this command to list AAA users and any method lists applied to them.

Syntax

```
show aaa server group
```

Mode Privileged Exec

Example To show the AAA configuration on a device, use the command:

```
awplus# aaa server group
```

Output Figure 31-2: Example output from **aaa server group**

```
awplus#show aaa server group
User          List Name     Method                  Acct-Event
======== ==== ============= ================ ======= ==========
login    auth default       -                local   -
-------- ---- ------------- ---------------- ------- ----------
login    acct -             -                -       -
-------- ---- ------------- ---------------- ------- ----------
dot1x    auth default       radius           group   -
dot1x    auth vlan30_auth   rad_group_1      group   -
dot1x    auth vlan40_auth   rad_group_2      group   -
-------- ---- ------------- ---------------- ------- ----------
dot1x    acct vlan30_acct   rad_group_4      group   start-stop
dot1x    acct vlan40_acct   rad_group_5      group   start-stop
-------- ---- ------------- ---------------- ------- ----------
auth-mac auth default       radius           group   -
auth-mac auth vlan10_auth   rad_group_vlan10 group   -
auth-mac auth vlan20_auth   rad_group_vlan20 group   -
-------- ---- ------------- ---------------- ------- ----------
auth-mac acct vlan10_acct   rad_group_vlan10 group   start-stop
auth-mac acct vlan20_acct   rad_group_vlan20 group   start-stop
-------- ---- ------------- ---------------- ------- ----------
auth-web auth default       radius           group   -
-------- ---- ------------- ---------------- ------- ----------
auth-web acct default       rad_group_3      group   start-stop
-------- ---- ------------- ---------------- ------- ----------
```

Related Commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting auth-mac

aaa authentication auth-web

aaa authentication dot1x

show debugging aaa

Overview This command displays the current debugging status for AAA (Authentication, Authorization, Accounting).

Syntax

```
show debugging aaa
```

Mode User Exec and Privileged Exec

Example To display the current debugging status of AAA, use the command:

```
awplus# show debug aaa
```

Output Figure 31-3: Example output from the **show debug aaa** command

```
AAA debugging status:
 Authentication debugging is on
 Accounting debugging is off
```

show radius server group

Overview Use this command to show the RADIUS server group configuration.

Syntax

```
show radius server group [<group-name>]
```

Parameter	Description
<group-name>	RADIUS server group name.

Default Command name is set to something by default.

Mode Privileged Exec

Usage Use this command with the *<group-name>* parameter to display information for a specific RADIUS server group, or without the parameter to display information for all RADIUS server groups.

Example To display information for all RADIUS server groups, use the command:

```
awplus# show radius server group
```

To display a information for a RADIUS server group named 'rad_group_vlan10', use the command:

```
awplus# show radius server group rad_group_vlan10
```

Output Figure 31-4: Example output from **show radius server group**

```
awplus#show radius server group
RADIUS Group Configuration
  Group Name : radius?
    Server Host/     Auth  Acct  Auth    Acct
    IP Address       Port  Port  Status  Status
    ----------------------------------------
    192.168.1.101    1812  1813  Active  Active
    192.168.1.102    1812  1813  Active  Active

  Group Name : rad_group_vlan10
    Server Host/     Auth  Acct  Auth    Acct
    IP Address       Port  Port  Status  Status
    ----------------------------------------
    192.168.1.101    1812  1813  Active  Active

  Group Name : rad_group_vlan20
    Server Host/     Auth  Acct  Auth    Acct
    IP Address       Port  Port  Status  Status
    ----------------------------------------
    192.168.1.102    1812  1813  Active  Active
```

Figure 31-5: Example output from **show radius server group rad_group_vlan10**

```
awplus#show radius server group rad_group_vlan10
RADIUS Group Configuration
  Group Name : rad_group_vlan10
    Server Host/    Auth  Acct  Auth    Acct
    IP Address      Port  Port  Status  Status
    ----------------------------------------
    192.168.1.101   1812  1813  Active  Active
```

Related Commands aaa group server

undebug aaa

Overview This command applies the functionality of the **no** debug aaa command.

32 RADIUS Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device to use RADIUS servers.

Command List

auth radius send nas-identifier

Overview Use this command to enable the device to include the NAS-Identifier(32) attribute in RADIUS authentication requests.

Use the **no** variant of this command to stop including the NAS-Identifier attribute.

Syntax

```
auth radius send nas-identifier [<name>|vlan-id]
no auth radius send nas-identifier
```

Parameter	Description
<name>	Send this user-defined text as the NAS-Identifier. You can specify up to 253 characters.
vlan-id	Send the VLAN ID of the authentication port as the NAS-Identifier. This is the configured VLAN ID, not the dynamic VLAN ID or guest VLAN ID.

Mode Global Configuration

Example To use a user-defined identifier of NASID100 as the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send nas-identifier NASID100
```

To use the VLAN ID as the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send nas-identifier vlan-id
```

To stop sending the NAS-Identifier attribute, use the commands:

```
awplus# configure terminal
awplus(config)# no auth radius send nas-identifier
```

Related Commands auth radius send service-type

auth radius send service-type

Overview Use this command to enable the device to include the Service-Type(6) attribute in RADIUS authentication requests. The Service-Type attribute has a value of:

- Framed(2) for 802.1x
- Call-Check(10) for MAC authentication
- Unbound(5) for Web authentication.

Use the **no** variant of this command to stop including the Service-Type attribute.

Syntax

```
auth radius send service-type
no auth radius send service-type
```

Mode Global Configuration

Example To send the Service-Type attribute, use the commands:

```
awplus# configure terminal
awplus(config)# auth radius send service-type
```

Related Commands auth radius send nas-identifier

deadtime (RADIUS server group)

Overview Use this command to configure the **deadtime** parameter for the RADIUS server group. This command overrides the global dead-time configured by the radius-server deadtime command. The configured deadtime is the time period in minutes to skip a RADIUS server for authentication or accounting requests if the server is “dead”. Note that a RADIUS server is considered “dead” if there is no response from the server within a defined time period.

Use the **no** variant of this command to reset the deadtime configured for the RADIUS server group. If the global deadtime for RADIUS server is configured the value will be used for the servers in the group. The global deadtime for the RADIUS server is set to 0 minutes by default.

Syntax

```
deadtime <0-1440>
no deadtime
```

Parameter	Description
<0-1440>	Amount of time in minutes.

Default The deadtime is set to 0 minutes by default.

Mode Server Group Configuration

Usage If the RADIUS server does not respond to a request packet, the packet is retransmitted the number of times configured for the **retransmit** parameter (after waiting for a **timeout** period to expire). The server is then marked “dead”, and the time is recorded. The **deadtime** parameter configures the amount of time to skip a dead server; if a server is dead, no request message is sent to the server for the **deadtime** period.

Examples To configure the deadtime for 5 minutes for the RADIUS server group “GROUP1”, use the command:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# server 192.168.1.1
awplus(config-sg)# deadtime 5
```

To remove the deadtime configured for the RADIUS server group “GROUP1”, use the command:

```
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no deadtime
```

Related Commands aaa group server

radius-server deadtime

debug radius

Overview This command enables RADIUS debugging. If no option is specified, all debugging options are enabled.

Use the **no** variant of this command to disable RADIUS debugging. If no option is specified, all debugging options are disabled.

Syntax

```
debug radius [packet|event|all]
no debug radius [packet|event|all]
```

Parameter	Description
`packet`	Debugging for RADIUS packets is enabled or disabled.
`event`	Debugging for RADIUS events is enabled or disabled.
`all`	Enable or disable all debugging options.

Default RADIUS debugging is disabled by default.

Mode Privileged Exec

Examples To enable debugging for RADIUS packets, use the command:

```
awplus#  debug radius packet
```

To enable debugging for RADIUS events, use the command:

```
awplus#  debug radius event
```

To disable debugging for RADIUS packets, use the command:

```
awplus# no debug radius packet
```

To disable debugging for RADIUS events, use the command:

```
awplus# no debug radius event
```

Related Commands show debugging radius

undebug radius

ip radius source-interface

Overview This command configures the source IP address of every outgoing RADIUS packet to use a specific IP address or the IP address of a specific interface. If the specified interface is down or there is no IP address on the interface, then the source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Use the **no** variant of this command to remove the source interface configuration. The source IP address in outgoing RADIUS packets will be the IP address of the interface from which the packets are sent.

Syntax

```
ip radius source-interface {<interface>|<ip-address>}
no ip radius source-interface
```

Parameter	Description
<interface>	Interface name.
<ip-address>	IP address in the dotted decimal format A.B.C.D.

Default Source IP address of outgoing RADIUS packets depends on the interface the packets leave.

Mode Global Configuration

Examples To configure all outgoing RADIUS packets to use the IP address of the interface “vlan1” for the source IP address, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface vlan1
```

To configure the source IP address of all outgoing RADIUS packets to use 192.168.1.10, use the following commands:

```
awplus# configure terminal
awplus(config)# ip radius source-interface 192.168.1.10
```

To reset the source interface configuration for all outgoing RADIUS packets, use the following commands:

```
awplus# configure terminal
awplus(config)# no ip radius source-interface
```

Related Commands radius-server host

show radius statistics

radius-server deadtime

Overview Use this command to specify the global **deadtime** for all RADIUS servers. If a RADIUS server is considered dead, it is skipped for the specified deadtime. This command specifies for how many minutes a RADIUS server that is not responding to authentication requests is passed over by requests for RADIUS authentication.

Use the **no** variant of this command to reset the global deadtime to the default of 0 seconds, so that RADIUS servers are not skipped even if they are dead.

Syntax

```
radius-server deadtime <minutes>
no radius-server deadtime
```

Parameter	Description
<minutes>	RADIUS server deadtime in minutes in the range 0 to 1440 (24 hours).

Default The default RADIUS deadtime configured on the system is 0 seconds.

Mode Global Configuration

Usage The RADIUS client considers a RADIUS server to be dead if it fails to respond to a request after it has been retransmitted as often as specified globally by the radius-server retransmit command or for the server by the radius-server host command. To improve RADIUS response times when some servers may be unavailable, set a **deadtime** to skip dead servers.

Examples To set the dead time of the RADIUS server to 60 minutes, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server deadtime 60
```

To disable the dead time of the RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server deadtime
```

Related Commands

deadtime (RADIUS server group)

radius-server host

radius-server retransmit

show radius statistics

radius-server host

Overview Use this command to specify a remote RADIUS server host for authentication or accounting, and to set server-specific parameters. The parameters specified with this command override the corresponding global parameters for RADIUS servers. This command specifies the IP address or host name of the remote RADIUS server host and assigns authentication and accounting destination UDP port numbers.

This command adds the RADIUS server address and sets parameters to the RADIUS server. The RADIUS server is added to the running configuration after you issue this command. If parameters are not set using this command then common system settings are applied.

Use the **no** variant of this command to remove the specified server host as a RADIUS authentication and/or accounting server and set the destination port to the default RADIUS server port number (1812).

Syntax

```
radius-server host {<host-name>|<ip-address>} [acct-port
<0-65535>] [auth-port <0-65535>] [key <key-string>] [retransmit
<0-100>] [timeout <1-1000>]
```

```
no radius-server host {<host-name>|<ip-address>} [acct-port
<0-65535>] [auth-port <0-65535>]
```

Parameter	Description
<host-name>	Server host name. The DNS name of the RADIUS server host.
<ip-address>	The IP address of the RADIUS server host.
`acct-port`	Accounting port. Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the server is not used for accounting. The default UDP port for accounting is 1813.
<0-65535>	UDP port number (Accounting port number is set to 1813 by default) Specifies the UDP destination port for RADIUS accounting requests. If 0 is specified, the host is not used for accounting.
`auth-port`	Authentication port. Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the server is not used for authentication. The default UDP port for authentication is 1812.
<0-65535>	UDP port number (Authentication port number is set to 1812 by default) Specifies the UDP destination port for RADIUS authentication requests. If 0 is specified, the host is not used for authentication.
`timeout`	Specifies the amount of time to wait for a response from the server. If this parameter is not specified the global value configured by the **radius-server timeout** command is used.

Parameter	Description
<1-1000>	Time in seconds to wait for a server reply (timeout is set to 5 seconds by default) The time interval (in seconds) to wait for the RADIUS server to reply before retransmitting a request or considering the server dead. This setting overrides the global value set by the **radius-server timeout** command. If no timeout value is specified for this server, the global value is used.
`retransmit`	Specifies the number of retries before skip to the next server. If this parameter is not specified the global value configured by the **radius-server retransmit** command is used.
<0-100>	Maximum number of retries (maximum number of retries is set to 3 by default) The maximum number of times to resend a RADIUS request to the server, if it does not respond within the timeout interval, before considering it dead and skipping to the next RADIUS server. This setting overrides the global setting of the **radius-server retransmit** command. If no retransmit value is specified, the global value is used.
`key`	Set shared secret key with RADIUS servers
<key-string>	Shared key string applied Specifies the shared secret authentication or encryption key for all RADIUS communications between this device and the RADIUS server. This key must match the encryption used on the RADIUS daemon. All leading spaces are ignored, but spaces within and at the end of the string are used. If spaces are used in the string, do not enclose the string in quotation marks unless the quotation marks themselves are part of the key. This setting overrides the global setting of the **radius-server key c** ommand. If no key value is specified, the global value is used.

Default The RADIUS client address is not configured (null) by default. No RADIUS server is configured.

Mode Global Configuration

Usage Multiple **radius -server host** commands can be used to specify multiple hosts. The software searches for hosts in the order they are specified. If no host-specific timeout, retransmit, or key values are specified, the global values apply to that host. If there are multiple RADIUS servers for this client, use this command multiple times—once to specify each server.

If you specify a host without specifying the auth port or the acct port, it will by default be configured for both authentication and accounting, using the default UDP ports. To set a host to be a RADIUS server for authentication requests only, set the **acct-port** parameter to 0; to set the host to be a RADIUS server for accounting requests only, set the auth-port parameter to 0.

A RADIUS server is identified by IP address, authentication port and accounting port. A single host can be configured multiple times with different authentication or accounting ports. All the RADIUS servers configured with this command are

included in the predefined RADIUS server group radius, which may be used by AAA authentication, authorization and accounting commands. The client transmits (and retransmits, according to the **retransmit** and **timeout** parameters) RADIUS authentication or accounting requests to the servers in the order you specify them, until it gets a response.

Examples To add the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20
```

To set the secret key to **allied** on the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 10.0.0.20 key allied
```

To delete the RADIUS server `10.0.0.20`, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host 10.0.0.20
```

To configure `rad1.company.com` for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad1.company.com acct-port 0
```

To remove the RADIUS server `rad1.company.com` configured for authentication only, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server host rad1.company.com
acct-port 0
```

To configure `rad2.company.com` for accounting only, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host rad2.company.com auth-port 0
```

To configure 192.168.1.1 with authentication port 1000, accounting port 1001 and retransmit count 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server host 192.168.1.1 auth-port 1000
acct-port 1001 retransmit 5
```

Related Commands

aaa group server

radius-server key

radius-server retransmit

radius-server timeout

show radius statistics

radius-server key

Overview This command sets a global secret key for RADIUS authentication on the device. The shared secret text string is used for RADIUS authentication between the device and a RADIUS server.

Note that if no secret key is explicitly specified for a RADIUS server, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to reset the secret key to the default (null).

Syntax

```
radius-server key <key>
no radius-server key
```

Parameter	Description
<key>	Shared secret among radius server and 802.1X client.

Default The RADIUS server secret key on the system is not set by default (null).

Mode Global Configuration

Usage Use this command to set the global secret key shared between this client and its RADIUS servers. If no secret key is specified for a particular RADIUS server using the **radius-server host c** ommand, this global key is used.

After enabling AAA authentication with the **aaa authentication login** command, set the authentication and encryption key using the **radius-server key** command so the key entered matches the key used on the RADIUS server.

Examples To set the global secret key to **allied** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key allied
```

To set the global secret key to **secret** for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server key secret
```

To delete the global secret key for RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server key
```

Related Commands radius-server host

show radius statistics

radius-server retransmit

Overview This command sets the retransmit counter to use RADIUS authentication on the device. This command specifies how many times the device transmits each RADIUS request to the RADIUS server before giving up.

This command configures the **retransmit** parameter for RADIUS servers globally. If the **retransmit** parameter is not specified for a RADIUS server by the **radius-server host** command then the global configuration set by this command is used for the server instead.

Use the **no** variant of this command to reset the re-transmit counter to the default (3).

Syntax

```
radius-server retransmit <retries>
no radius-server retransmit
```

Parameter	Description
<retries>	RADIUS server retries in the range <0-100>. The number of times a request is resent to a RADIUS server that does not respond, before the server is considered dead and the next server is tried. If no retransmit value is specified for a particular RADIUS server using the **radius-server host** command, this global value is used.

Default The default RADIUS retransmit count on the device is 3.

Mode Global Configuration

Examples To set the RADIUS **retransmit** count to 1, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 1
```

To set the RADIUS **retransmit** count to the default (3), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server retransmit
```

To configure the RADIUS **retransmit** count globally with 5, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 5
```

To disable retransmission of requests to a RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server retransmit 0
```

Related Commands

radius-server deadtime

radius-server host

show radius statistics

radius-server timeout

Overview Use this command to specify the RADIUS global timeout value. This is how long the device waits for a reply to a RADIUS request before retransmitting the request, or considering the server to be dead. If no timeout is specified for the particular RADIUS server by the **radius-server host** command, it uses this global timeout value.

Note that this command configures the **timeout** parameter for RADIUS servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
radius-server timeout <seconds>
no radius-server timeout
```

Parameter	Description
<seconds>	RADIUS server timeout in seconds in the range 1 to 1000. The global time in seconds to wait for a RADIUS server to reply to a request before retransmitting the request, or considering the server to be dead (depending on the **radius-server retransmit** command).

Default The default RADIUS transmit timeout on the system is 5 seconds.

Mode Global Configuration

Examples To globally set the device to wait 20 seconds before retransmitting a RADIUS request to unresponsive RADIUS servers, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 20
```

To set the RADIUS **timeout** parameter to 1 second, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 1
```

To set the RADIUS **timeout** parameter to the default (5 seconds), use the following commands:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

To configure the RADIUS server **timeout** period globally with 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server timeout 3
```

To reset the global **timeout** period for RADIUS servers to the default, use the following command:

```
awplus# configure terminal
awplus(config)# no radius-server timeout
```

Related Commands

radius-server deadtime

radius-server host

radius-server retransmit

show radius statistics

server (Server Group)

Overview This command adds a RADIUS server to a server group in Server-Group Configuration mode. The RADIUS server should be configured by the radius-server host command.

The server is appended to the server list of the group and the order of configuration determines the precedence of servers. If the server exists in the server group already, it will be removed before added as a new server.

The server is identified by IP address and authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports. The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set `auth-port` to 0. If the authentication port is missing, the default port number is 1812. The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set `acct-port` to 0. If the accounting port is missing, the default port number is 1812.

Use the **no** variant of this command to remove a RADIUS server from the server group.

Syntax

```
server {<hostname>|<ip-address>} [auth-port
<0-65535>][acct-port <0-65535>]
```

```
no server {<hostname>|<ip-address>} [auth-port
<0-65535>][acct-port <0-65535>]
```

Parameter	Description
<hostname>	Server host name
<ip-address>	Server IP address The server is identified by IP address, authentication and accounting UDP port numbers. So a RADIUS server can have multiple entries in a group with different authentication and/or accounting UDP ports.
`auth-port`	Authentication port The **auth-port** specifies the UDP destination port for authentication requests to the server. To disable authentication for the server, set **auth-port** to 0. If the authentication port is missing, the default port number is 1812.
<0-65535>	UDP port number (default: 1812)
`acct-port`	Accounting port The **acct-port** specifies the UDP destination port for accounting requests to the server. To disable accounting for the server, set **acct-port** to 0. If the accounting port is missing, the default port number is 1813.
<0-65535>	UDP port number (default: 1813)

Default The default Authentication port number is 1812 and the default Accounting port number is 1813.

Mode Server Group Configuration

Usage The RADIUS server to be added must be configured by the **radius-server host** command. In order to add or remove a server, the **auth-port** and **acct-port** parameters in this command must be the same as the corresponding parameters in the **radius-server host** command.

Examples To create a RADIUS server group RAD_AUTH1 for authentication, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_AUTH1
awplus(config-sg)# server 192.168.1.1 acct-port 0
awplus(config-sg)# server 192.168.2.1 auth-port 1000 acct-port
0
```

To create a RADIUS server group RAD_ACCT1 for accounting, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius RAD_ACCT1
awplus(config-sg)# server 192.168.2.1 auth-port 0 acct-port
1001
awplus(config-sg)# server 192.168.3.1 auth-port 0
```

To remove server 192.168.3.1 from the existing server group **GROUP1**, use the following commands:

```
awplus# configure terminal
awplus(config)# aaa group server radius GROUP1
awplus(config-sg)# no server 192.168.3.1
```

Related Commands

aaa accounting auth-mac

aaa accounting auth-web

aaa accounting dot1x

aaa accounting login

aaa authentication auth-mac

aaa authentication auth-web

aaa authentication login

aaa group server

radius-server host

show debugging radius

Overview This command displays the current debugging status for the RADIUS servers.

Syntax

```
show debugging radius
```

Mode User Exec and Privileged Exec

Example To display the current debugging status of RADIUS servers, use the command:

```
awplus# show debugging radius
```

Output Figure 32-1: Example output from the **show debugging radius** command

```
RADIUS debugging status:
 RADIUS event debugging is off
 RADIUS packet debugging is off
```

show radius

Overview This command displays the current RADIUS server configuration and status.

Syntax

```
show radius
```

Mode User Exec and Privileged Exec

Example To display the current status of RADIUS servers, use the command:

```
awplus# show radius
```

Output Figure 32-2: Example output from the **show radius** command showing RADIUS servers

```
RADIUS Global Configuration
 Source Interface : not configured
 Secret Key : secret
 Timeout : 5 sec
 Retransmit Count : 3
 Deadtime : 20 min
Server Host : 192.168.1.10
 Authentication Port : 1812
 Accounting Port : 1813
 Secret Key : secret
 Timeout : 3 sec
 Retransmit Count : 2
Server Host : 192.168.1.11
 Authentication Port : 1812
 Accounting Port : not configured

Server Name/   Auth   Acct   Auth     Acct
IP Address     Port   Port   Status   Status
-----------------------------------------------------------
192.168.1.10   1812   1813   Alive    Alive
192.168.1.11   1812   N/A    Alive    N/A
```

Example See the sample output below showing RADIUS client status and RADIUS configuration:

```
awplus# show radius
```

Output Figure 32-3: Example output from the **show radius** command showing RADIUS client status

```
RADIUS global interface name: awplus
 Secret key:
 Timeout: 5
 Retransmit count: 3
 Deadtime: 0

Server Address: 150.87.18.89
 Auth destination port: 1812
 Accounting port: 1813
 Secret key: swg
 Timeout: 5
 Retransmit count: 3
 Deadtime: 0show radius local-server group
```

Output Parameter	Meaning
Source Interface	The interface name or IP address to be used for the source address of all outgoing RADIUS packets.
Secret Key	A shared secret key to a radius server.
Timeout	A time interval in seconds.
Retransmit Count	The number of retry count if a RADIUS server does not response.
Deadtime	A time interval in minutes to mark a RADIUS server as “dead”.
Interim-Update	A time interval in minutes to send Interim-Update Accounting report.
Group Deadtime	The deadtime configured for RADIUS servers within a server group.
Server Host	The RADIUS server hostname or IP address.
Authentication Port	The destination UDP port for RADIUS authentication requests.
Accounting Port	The destination UDP port for RADIUS accounting requests.

Output Parameter	Meaning	
`Auth Status`	The status of the authentication port. The status ("dead", "error", or "alive") of the RADIUS authentication server and, if dead, how long it has been dead for.	
	`Alive`	The server is alive.
	`Error`	The server is not responding.
	`Dead`	The server is detected as dead and it will not be used for deadtime period. The time displayed in the output shows the server is in dead status for that amount of time.
	`Unknown`	The server is never used or the status is unknown.
`Acct Status`	The status of the accounting port. The status ("dead", "error", or "alive") of the RADIUS accounting server and, if dead, how long it has been dead for.	

show radius statistics

Overview This command shows the RADIUS client statistics for the device.

Syntax

```
show radius statistics
```

Mode User Exec and Privileged Exec

Example See the sample output below showing RADIUS client statistics and RADIUS configuration:

```
awplus# show radius statistics
```

Output Figure 32-4: Example output from the **show radius statistics** command:

```
RADIUS statistics for Server: 150.87.18.89
 Access-Request Tx  : 5 - Retransmit  : 0
 Access-Accept Rx  : 1 - Access-Reject Rx  : 2
 Access-Challenge Rx  : 2
 Unknown Type  : 0 - Bad Authenticator : 0
 Malformed Access-Resp : 0 - Wrong Identifier : 0
 Bad Attribute  : 0 - Packet Dropped  : 0
 TimeOut  : 0 - Dead count  : 0
 Pending Request : 0
```

undebug radius

Overview This command applies the functionality of the **no** debug radius command.

33 Local RADIUS Server Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the local RADIUS server on the device. For more information, see the Local RADIUS Server Feature Overview and Configuration Guide.

Command List

attribute

Overview Use this command to define a RADIUS attribute for the local RADIUS server user group.

For a complete list of defined RADIUS attributes and values, see the Local RADIUS Server Feature Overview and Configuration Guide.

When used with the **help** parameter the **attribute** command displays a list of standard and vendor specific valid RADIUS attributes that are supported by the local RADIUS server.

If an attribute name is specified with the **help** parameter, then the **attribute** command displays a list of predefined attribute names. Note that you can only use the defined RADIUS attribute names and not define your own.

When used with the **value** parameter the **attribute** command configures RADIUS attributes to the user group. If the specified attribute is already defined then it is replaced with the new value.

Use the **no** variant of this command to delete an attribute from the local RADIUS server user group.

Syntax

```
attribute [<attribute-name>|<attribute-id>] help
attribute {<attribute-name>|<attribute-id>} <value>
no attribute {<attribute-name>|<attribute-id>}
```

Parameter	Description
<attribute-name>	RADIUS attribute name for standard attributes or Vendor-Specific attributes (see the Local RADIUS Server Feature Overview and Configuration Guide for tables of attributes).
<attribute-id>	RADIUS attribute numeric identifier for standard attributes.
<value>	RADIUS attribute value.
`help`	Display a list of available attribute types.

Default By default, no attributes are configured.

Mode RADIUS Server Group Configuration

Usage For the Standard attributes, the attribute may be specified using either the attribute name, or its numeric identifier. For example, the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause
help
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 help
```

In the same way, where the specific attribute has a pre-defined value, the parameter <*value*> may be substituted with the Value Name or with its numeric value, for example the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause
user-request
```

will produce the same results as the command:

```
awplus(config-radsrv-group)# attribute 49 1
```

or the command:

```
awplus(config-radsrv-group)# attribute acct-terminate-cause 1
```

Examples To check a list of all available defined RADIUS attribute names, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute help
```

A list of Vendor-specific Attributes displays after the list of defined Standard Attributes.

To get help for valid RADIUS attribute values for the attribute `Service-Type`, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute Service-Type help
```

This results in the following output:

```
Service-Type : integer (Integer number)

Pre-defined values :
    Administrative-User (6)
    Authenticate-Only (8)
    Authorize-Only (17)
    Callback-Administrative (11)
    Callback-Framed-User (4)
    Callback-Login-User (3)
    Callback-NAS-Prompt (9)
    Call-Check (10)
    Framed-User (2)
    Login-User (1)
    NAS-Prompt-User (7)
    Outbound-User (5)
```

To define the attribute name 'Service-Type' with Administrative User (6) to the RADIUS User Group 'Admin', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# attribute Service-Type 6
```

To delete the attribute 'Service-Type' from the RADIUS User Group 'Admin', use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group Admin
awplus(config-radsrv-group)# no attribute Service-Type
```

Related Commands

egress-vlan-id

egress-vlan-name

authentication

Overview Use this command to enable the specified authentication methods on the local RADIUS server.

Use the **no** variant of this command to disable specified authentication methods on the local RADIUS server.

Syntax

```
authentication {mac|eapmd5|eaptls|peap}
no authentication {mac|eapmd5|eaptls|peap}
```

Parameter	Description
`mac`	Enable MAC authentication method.
`eapmd5`	Enable EAP-MD5 authentication method.
`eaptls`	Enable EAP-TLS authentication method.
`peap`	Enable EAP-PEAP authentication method.

Default All authentication methods are enabled by default.

Mode RADIUS Server Configuration

Examples The following commands enable EAP-MD5 authentication methods on the local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# authentication eapmd5
```

The following commands disable EAP-MD5 authentication methods on Local RADIUS server.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no authentication eapmd5
```

Related Commands server enable

show radius local-server statistics

clear radius local-server statistics

Overview Use this command to clear the statistics stored on the device for the local RADIUS server.

Use this command without any parameters to clear all types of local RADIUS server statistics.

Syntax

```
clear radius local-server statistics [nas|server|user]
```

Parameter	Description
`nas`	Clear the NAS (Network Access Server) statistics on the device. For example, clearing statistics stored for NAS server invalid passwords.
`server`	Clear the Local RADIUS Server statistics on the device. For example, clearing Local RADIUS Servers statistics for all failed login attempts.
`user`	Clear the Local RADIUS Server user statistics. For example, clearing statistics stored for the number of successful user logins.

Mode Privileged Exec

Usage Refer to the sample output for the show radius local-server statistics for further information about the type of statistics each parameter option for this command clears. Both the **nas** and **server** parameters clear unknown username and invalid passwords statistics, while the `user` parameter clears the number of successful and failed logins for each local RADIUS server user.

Examples To clear the NAS (Network Access Server) statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics nas
```

To clear the local RADIUS server statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics server
```

To clear the local RADIUS server user statistics stored on the device, use the command:

```
awplus# clear radius local-server statistics user
```

Related Commands show radius local-server statistics

copy fdb-radius-users (to file)

Overview Use this command to create a set of local RADIUS server users from MAC addresses in the local FDB. A local RADIUS server user created using this command can be used for MAC authentication.

Syntax

```
copy fdb-radius-users
{local-radius-user-db|flash|nvs|usb|debug|tftp|scp|
fserver|<url>} [interface <port>] [vlan <vid>] [group <name>]
[export-vlan [<radius-group-name>]]
```

Parameter	Description
`local-radius-user-db`	Copy the local RADIUS server users created to the local RADIUS server.
`flash`	Copy the local RADIUS server users created to Flash memory.
`nvs`	Copy the local RADIUS server users created to NVS memory.
`usb`	Copy the local RADIUS server users created to USB storage device.
`debug`	Copy the local RADIUS server users created to debug.
`tftp`	Copy the local RADIUS server users created to the TFTP destination.
`scp`	Copy the local RADIUS server users created to the SCP destination.
`fserver`	Copy the local RADIUS server users created to the remote file server.
`<url>`	Copy the local RADIUS server users created to the specified URL.
`interface <port>`	Copy only MAC addresses learned on a specified device port. Wildcards may be used when specifying an interface name.For example, when you specify interface port1.* then this command generates RADIUS server users for MAC addresses learned on stack 1.
`vlan <vid>`	Copy only MAC addresses learned on a specified VLAN.
`group <name>`	Assign a group name to the local RADIUS server users created.
`export-vlan`	Export VLAN ID assigned to exported FDB entry.
`<radius-group-name>`	Prefix for Radius group name storing VLAN ID

Mode Privileged Exec

Usage The local RADIUS server users created are written to a specified destination file in local RADIUS user CSV (Comma Separated Values) format. The local RADIUS server

users can then be imported to a local RADIUS server using the copy local-radius-user-db (from file) command.

The name and password of the local RADIUS server users created use a MAC address, which can be used for MAC authentication.

This command does not copy a MAC address learned by the CPU or the management port.

This command can filter FDB entries by the interface name and the VLAN ID. When the interface name and the VLAN ID are specified, this command generates local RADIUS server users from only the MAC address learned on the specified interface and on the specified VLAN.

Examples To register the local RADIUS server users from the local FDB directly to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db
```

To register the local RADIUS server users from the interface `port1.0.1` to the local RADIUS server, use the command:

```
awplus# copy fdb-radius-users local-radius-user-db interface
port1.0.1
```

To copy output generated as local RADIUS server user data from MAC addresses learned on `vlan10` on interface `port1.0.1` to the file `radius-user.csv`, use the command:

```
awplus# copy fdb-radius-users radius-user.csv interface
port1.0.1 vlan10
```

To copy output generated as local RADIUS server user data from MAC addresses learned on `vlan10` on interface `port1.0.1` to a file on the remote file server, use the command:

```
awplus# copy fdb-radius-users fserver interface port1.0.1
vlan10
```

Related Commands copy local-radius-user-db (to file)

copy local-radius-user-db (from file)

copy local-radius-user-db (from file)

Overview Use this command to copy the Local RADIUS server user data from a file. The file, including the RADIUS user data in the file, must be in the CSV (Comma Separated Values) format.

You can select **add** or **replace** as the copy method. The **add** parameter option copies the contents of specified file to the local RADIUS server user database. If the same user exists then the old user is removed before adding a new user. The **replace** parameter option deletes all contents of the local RADIUS server user database before copying the contents of specified file.

Syntax

```
copy <source-url> local-radius-user-db [add|replace]
```

Parameter	Description
<source-url>	URL of the source file.
`add`	Add file contents to local RADIUS server user database.
`replace`	Replace current local RADIUS server user database with file contents.

Default When no copy method is specified with this command the **replace** option is applied.

Mode Privileged Exec

Examples To replace the current local RADIUS server user data to the contents of http://datahost/ user.csv, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db
```

To add the contents of http://datahost/user.csv to the current local RADIUS server user database, use the following command:

```
awplus# copy http://datahost/user.csv local-radius-user-db add
```

Related commands copy fdb-radius-users (to file)

copy local-radius-user-db (to file)

copy local-radius-user-db (to file)

Overview Use this command to copy the local RADIUS server user data to a file. The output file produced is CSV (Comma Separated Values) format.

Syntax

```
copy local-radius-user-db
{flash|nvs|usb|tftp|scp|<destination-url>}
```

Parameter	Description
`flash`	Copy to flash memory.
`nvs`	Copy to NVS memory.
`usb`	Copy to USB storage device.
`tftp`	Copy to TFTP destination.
`scp`	Copy to SCP destination.
<destination-url>	URL of the Destination file.

Mode Privileged Exec

Example Copy the current local RADIUS server user data to http://datahost/user.csv.

```
awplus# copy local-radius-user-db http://datahost/user.csv
```

Related Commands

copy fdb-radius-users (to file)

copy local-radius-user-db (from file)

crypto pki enroll local

Overview Use this command to obtain a system certificate from the Local CA (Certificate Authority).

Use the **no** variant of this command to delete system certificates created by a Local CA (Certificate Authority).

Syntax

```
crypto pki enroll local
no crypto pki enroll local
```

Default The system certificate is not available until this command is issued.

Mode Global Configuration

Examples The following command obtains the system certificate from the Local CA (Certificate Authority).

```
awplus# configure terminal
awplus(config)# crypto pki enroll local
```

The following command deletes the system certificate created by the Local CA (Certificate Authority).

```
awplus# configure terminal
awplus(config)# no crypto pki enroll local
```

Related Commands crypto pki trustpoint local

group

crypto pki enroll local local-radius-all-users

Overview Use this command to create certificates for all users registered in the local RADIUS server. These certificates are created by the Local Certificate Authority (CA) on the device.

Syntax
```
crypto pki enroll local local-radius-all-users
```

Default By default, there are no certificates for users in the local RADIUS server.

Mode Global Configuration

Example The following command obtains the local RADIUS server certificates for the user from the Local CA (Certificate Authority).

```
awplus# configure terminal
awplus(config)# crypto pki enroll local local-radius-all-users
```

Related Commands
crypto pki trustpoint local

show crypto pki certificates

crypto pki enroll local user

Overview Use this command to obtain a local user certificate from the Local CA (Certificate Authority).

Use the **no** variant of this command to delete user certificates created by the Local CA (Certificate Authority).

Syntax

```
crypto pki enroll local user <user-name>
no crypto pki enroll local user <user-name>
```

Parameter	Description
<user-name>	User name.

Default By default, there is no user certificate.

Mode Global Configuration

Examples The following command obtains Tom's certificate from the Local CA (Certificate Authority).

```
awplus# configure terminal
awplus(config)# crypto pki enroll local user Tom
```

The following command deletes Tom's certificates created by the Local CA (Certificate Authority):

```
awplus# configure terminal
awplus(config)# no crypto pki enroll local user Tom
```

Related Commands crypto pki trustpoint local

show crypto pki certificates

crypto pki export local pem

Overview Use this command to export the certificate associated with the Local CA to a PEM format file.

Syntax

```
crypto pki export local pem url <url>
```

Parameter	Description
<url>	URL string.

Mode Global Configuration

Example The following command exports the Local CA certificate to a PEM format file.

```
awplus# configure terminal
awplus(config)# crypto pki export local pem url
tftp://192.168.1.1/cacert.pem
```

Related Commands crypto pki enroll local

crypto pki export local pkcs12

Overview Use this command to export a specified certificate to a PKCS12 format file.

This command cannot be used for exporting certificates for the local system.

Syntax

```
crypto pki export local pkcs12 <user-name> <destination-url>
```

Parameter	Description
<user-name>	User name.
<destination-url>	Destination URL string.

Mode Global Configuration

Examples The following commands exports a certificate for a user named **client** to a PKCS12 format file.

```
awplus# configure terminal
awplus(config)# crypto pki export local pkcs12 client
tftp://192.168.1.1/cacert.pem
```

To export Tom's certificate to PKSC12 format file, use the commands:

```
awplus# configure terminal
awplus(config)# crypto pki export local pksc12 Tom
tftp://192.168.1.1/tom.pfx
```

Related Commands crypto pki enroll local

crypto pki trustpoint local

Overview Use this command to declare the Local CA (Certificate Authority) as the trustpoint that the system uses. The ca-trustpoint configuration mode is available after this command is issued.

Use the **no** variant of this command to delete all information and certificates associated with Local CA as the trustpoint.

Syntax
```
crypto pki trustpoint local
no crypto pki trustpoint local
```

Default Local CA is not a trustpoint.

Mode Global Configuration

Examples Use the following commands to declare the Local CA as the trustpoint.

```
awplus# configure terminal
awplus(config)# crypto pki trustpoint local
```

Use the following commands to delete all information and certificates associated with the Local CA.

```
awplus# configure terminal
awplus(config)# no crypto pki trustpoint local
```

To create a client certificate for all users registered to the local RADIUS server, use the following commands:

```
awplus(config)# crypto pki trustpoint local
awplus(ca-trust-point)# exit
awplus(config)# crypto pki enroll local alternative
```

Related Commands
crypto pki enroll local

show crypto pki trustpoints

debug crypto pki

Overview Use this command to enable Public Key Infrastructure (PKI) debugging. When PKI debugging is enabled, the PKI module starts generating diagnostic messages to the system log.

Use the **no** variant of this command to disable Public Key Infrastructure (PKI) debugging. When PKI debugging is disabled, the PKI module stops generating diagnostic messages to the system log.

Syntax

```
debug crypto pki
no debug crypto pki
```

Default PKI debugging is disabled by default

Mode Privileged Exec

Examples To enable the PKI debugging facility, use the command:

```
awplus# debug crypto pki
```

To disable the PKI debugging facility, use the command:

```
awplus# no debug crypto pki
```

domain-style

Overview Use this command to enable a specified domain style on the local RADIUS server. The local RADIUS server decodes the domain portion of a username login string when this command is enabled.

Use the **no** variant of this command to disable the specified domain style on the local RADIUS server.

Syntax

```
domain-style {suffix-atsign|ntdomain}
```

Parameter	Description
`suffix-atsign`	Enable at sign "@" delimited suffix style, i.e. "user@domain".
`ntdomain`	Enable NT domain style, i.e. "domain\user".

Default This feature is disabled by default.

Mode RADIUS Server Configuration

Usage When both domain styles are enabled, the first domain style configured has the highest priority. A username login string is matched against the first domain style enabled. Then, if the username login string is not decoded, it is matched against the second domain style enabled.

Examples To enable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# domain-style ntdomain
```

To disable NT domain style on the local RADIUS server, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no domain-style ntdomain
```

Related Commands server enable

egress-vlan-id

Overview Use this command to configure the standard RADIUS attribute "Egress-VLANID (56)" for the local RADIUS Server user group.

Use the **no** variant of this command to remove the Egress-VLANID attribute from the local RADIUS server user group.

Syntax

```
egress-vlan-id <vid> [tagged|untagged]
no egress-vlan-id
```

Parameter	Description
`<vid>`	The VLAN identifier to be used for the Egress VLANID attribute, in the range 1 to 4094.
`tagged`	Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.
`untagged`	Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.

Default By default, no Egress-VLANID attributes are configured.

Mode RADIUS Server Group Configuration

Usage When a Voice VLAN is configured for dynamic VLAN allocation (switchport voice vlan command), the RADIUS server must be configured to send the VLAN information when an IP phone is successfully authenticated. Use either the egress-vlan-id command or the egress-vlan-name command, and specify the **tagged** parameter.

Examples To set the "Egress-VLANID" attribute for the *NormalUsers* local RADIUS server user group to VLAN identifier 200, with tagged frames, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-id 200 tagged
```

To remove the "Egress-VLANID" attribute for the *NormalUsers* local RADIUS server user group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-id
```

Related Commands

attribute

egress-vlan-name

switchport voice vlan

egress-vlan-name

Overview Use this command to configure the standard RADIUS attribute "Egress-VLAN-Name (58)" for the local RADIUS server user group.

Use the **no** variant of this command to remove the Egress-VLAN-Name attribute from the local RADIUS server user group.

Syntax

```
egress-vlan-name <vlan-name> [tagged|untagged]
no egress-vlan-name
```

Parameter	Description
`<vlan-name>`	The VLAN name to be configured as the Egress-VLAN-Name attribute.
`tagged`	Set frames on the VLAN as tagged. This sets the tag indication field to indicate that all frames on this VLAN are tagged.
`untagged`	Set all frames on the VLAN as untagged. This sets the tag indication field to indicate that all frames on this VLAN are untagged.

Default By default, no Egress-VLAN-Name attributes are configured.

Mode RADIUS Server Group Configuration

Usage When a Voice VLAN is configured for dynamic VLAN allocation (switchport voice vlan command), the RADIUS server must be configured to send the VLAN information when an IP phone is successfully authenticated. Use either the egress-vlan-id command or the egress-vlan-name command, and specify the **tagged** parameter.

Examples To configure the "Egress-VLAN-Name" attribute for the RADIUS server user group *NormalUsers* with the VLAN name *vlan2* and all frames on this VLAN tagged, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# egress-vlan-name vlan2 tagged
```

To delete the "Egress-VLAN-Name" attribute for the *NormalUsers* group, use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no egress-vlan-name
```

Related Commands

attribute

egress-vlan-id

switchport voice vlan

group

Overview Use this command to create a local RADIUS server user group, and enter local RADIUS Server User Group Configuration mode.

Use the **no** variant of this command to delete the local RADIUS server user group.

Syntax

```
group <user-group-name>
no group <user-group-name>
```

Parameter	Description
<user-group-name>	User group name string.

Mode RADIUS Server Configuration

Examples The following command creates the user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
```

The following command deletes user group NormalUsers.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no group NormalUsers
```

Related Commands

user (RADIUS server)

show radius local-server user

vlan (RADIUS server)

nas

Overview This command adds a client device (the Network Access Server or the NAS) to the list of devices that are able to send authentication requests to the local RADIUS server. The NAS is identified by its IP address and a shared secret (also referred to as a shared key) must be defined that the NAS will use to establish its identity.

Use the **no** variant of this command to remove a NAS client from the list of devices that are allowed to send authentication requests to the local RADIUS server.

Syntax

```
nas <ip-address> key <nas-keystring>
no nas <ip-address>
```

Parameter	Description
<ip-address>	RADIUS NAS IP address.
<nas-keystring>	NAS shared keystring.

Mode RADIUS Server Configuration

Examples The following commands add the NAS with an IP address of `192.168.1.2` to the list of clients that may send authentication requests to the local RADIUS server. Note the shared key that this NAS will use to establish its identify is `NAS_PASSWORD`.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# nas 192.168.1.2 key NAS_PASSWORD
```

The following commands remove the NAS with an IP address of `192.168.1.2` from the list of clients that are allowed to send authentication requests to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no nas 192.168.1.2
```

Related Commands show radius local-server nas

radius-server local

Overview Use this command to navigate to the Local RADIUS server configuration mode `(config-radsrv)` from the Global Configuration mode `(config)`.

Syntax
```
radius-server local
```

Mode Global Configuration

Example Local RADIUS Server commands are available from `config-radsrv` configuration mode. To change mode from User Exec mode to the Local RADIUS Server mode (config- radsrv), use the commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)#
```

Output

```
awplus(config)#radius-server local
Creating Local CA repository.....OK
Enrolling Local System to local trustpoint..OK
awplus(config-radsrv)#
```

Related Commands

server enable

show radius local-server group

show radius local-server nas

show radius local-server statistics

show radius local-server user

server auth-port

Overview Use this command to change the UDP port number for local RADIUS server authentication.

Use the **no** variant of this command to reset the RADIUS server authentication port back to the default.

Syntax

```
server auth-port <1-65535>
no server auth-port
```

Parameter	Description
<1-65535>	UDP port number.

Default The default local RADIUS server UDP authentication port number is 1812.

Mode RADIUS Server Configuration

Examples The following commands set the RADIUS server authentication port to 10000.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server auth-port 10000
```

The following commands reset the RADIUS server authentication port back to the default UDP port of 1812.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server auth-port
```

Related Commands server enable

show radius local-server statistics

server enable

Overview This command enables the local RADIUS server. The local RADIUS server feature is started immediately when this command is issued.

The **no** variant of this command disables local RADIUS server. When this command is issued, the local RADIUS server stops operating.

Syntax

```
server enable
no server enable
```

Default The local RADIUS server is disabled by default and must be enabled for use with this command.

Mode RADIUS Server Configuration

Examples To enable the local RADIUS server, use the following commands:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# server enable
```

To disable the local RADIUS server, use the command:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no server enable
```

Related Commands server auth-port

show radius local-server statistics

show crypto pki certificates

Overview Use this command to display certificate information for Local CA and Local System certificates.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show crypto pki certificates [local-ca|local]
```

Parameter	Description
`local-ca`	Local CA certificate.
`local`	Local system certificate.

Mode User Exec and Privileged Exec

Examples The following command displays Local CA (Certificate Authority) certificate information.

```
awplus# show crypto pki certificates local-ca
```

The following command displays Local System certificate information.

```
awplus# show crypto pki certificates local
```

The following command displays information for all Local CA and Local System certificates.

```
awplus# show crypto pki certificates
```

Output

Table 1: Example output from the **show crypto pki certificates** command showing Local System and Local CA certificates

```
awplus#show crypto pki certificates
Certificate: Local System
    Data:
        Version: 3 (0x2)
        Serial Number: 4 (0x4)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
        Validity
            Not Before: Oct  8 07:50:55 2009 GMT
            Not After : Oct  6 07:50:55 2019 GMT
        Subject: O=Allied-Telesis, CN=Tom
Certificate: Local CA
    Data:
        Version: 3 (0x2)
        Serial Number: 0 (0x0)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
        Validity
            Not Before: Oct  8 07:55:55 2009 GMT
            Not After : Oct  6 07:55:55 2019 GMT
        Subject: O=Allied-Telesis, CN=Tom
```

Table 2: Parameters in the output of the **show crypto pki certificates** command

Parameter	Description
`Certificate`	Certificate name.
`Version`	Protocol version.
`Serial Number`	Serial number of the certificate.
`Signature Algorithm`	Algorithm used for the certificate signature.
`Issuer`	Subject of issuer creating the certificate.
`Validity`	Validity period.
`Subject`	Subject of the certificate.

Related Commands

crypto pki enroll local

show crypto pki certificates local-radius-all-users

Overview Use this command to display certificate information for local RADIUS server users.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show crypto pki certificates local-radius-all-users
```

Mode User Exec and Privileged Exec

Example The following command displays information of all local RADIUS server user certificates.

```
awplus# show crypto pki certificates local-radius-all-users
```

Output

Table 3: Example output from the **show crypto pki certificates local-radius-all-users** command

```
awplus#show crypto pki certificates local-radius-all-users
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
        Validity
            Not Before: Oct  8 07:50:55 2009 GMT
            Not After : Oct  6 07:50:55 2019 GMT
        Subject: O=Allied-Telesis, CN=Tom
```

Table 4: Parameters in the output of the **show crypto pki certificates local-radius- all-users** command

Parameter	Description
`Certificate`	Certificate name.
`Version`	Protocol version.
`Serial Number`	Serial number of the certificate.
`Signature Algorithm`	Algorithm used for the certificate signature.
`Issuer`	Subject of issuer creating the certificate.

Table 4: Parameters in the output of the **show crypto pki certificates local-radius- all-users** command (cont.)

Parameter	Description
`Validity`	Validity period.
`Subject`	Subject of the certificate.

Related Commands crypto pki enroll local local-radius-all-users

show crypto pki certificates user

Overview Use this command to display certificate information for a specified local RADIUS server user.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show crypto pki certificates user [<user-name>]
```

Parameter	Description
<user-name>	User name.

Mode User Exec and Privileged Exec

Example The following command displays Tom's certificate information.

```
awplus# show crypto pki certificates user Tom
```

Output

Table 5: Example output from the **show crypto pki certificates user** command to show certificate information for user Tom

```
awplus#show crypto pki certificates user Tom
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number: 2 (0x2)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: O=Allied-Telesis, CN=AlliedwarePlusCA
        Validity
            Not Before: Oct  8 07:50:55 2009 GMT
            Not After : Oct  6 07:50:55 2019 GMT
        Subject: O=Allied-Telesis, CN=Tom
```

Table 6: Parameters in the output of the **show crypto pki certificates user** command

Parameter	Description
`Certificate`	Certificate name.
`Version`	Protocol version.
`Serial Number`	Serial number of the certificate.

Table 6: Parameters in the output of the **show crypto pki certificates user** command (cont.)

Parameter	Description
`Signature Algorithm`	Algorithm used for the certificate signature.
`Issuer`	Subject of issuer creating the certificate.
`Validity`	Validity period.
`Subject`	Subject of the certificate.

Related Commands crypto pki enroll local user

show crypto pki trustpoints

Overview Use this command to display trustpoint information.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show crypto pki trustpoints
```

Mode User Exec and Privileged Exec

Example The following command displays trustpoint information.

```
awplus# show crypto pki trustpoint
```

Output

Table 7: Example output from the **show crypto pki trustpoints** command

```
Trustpoint local:
Subject Name:
CN = AlliedwarePlusCA
o = Allied-Telesis
Serial Number:0C
```

Table 8: Parameters in the output of the **show crypto pki trustpoints** command

Parameter	Description
Subject Name	CA certificate subject.
Serial Number	Current serial number of CA.

Related Commands crypto pki enroll local

show radius local-server group

Overview Use this command to display information about the local RADIUS server user group.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show radius local-server group [<user-group-name>]
```

Parameter	Description
<user-group-name>	User group name string.

Mode User Exec and Privileged Exec

Example The following command displays Local RADIUS server user group information.

```
awplus# show radius local-server group
```

Output

Table 9: Example output from the **show radius local-server group** command

```
Group-Name          Vlan
-------------------------------------------------------------------
NetworkOperators    ManagementNet
NormalUsers         CommonNet
```

Table 10: Parameters in the output of the **show radius local-server group** command

Parameter	Description
Group-Name	Group name.
Vlan	VLAN name assigned to the group.

Related Commands group

show radius local-server nas

Overview Use this command to display information about NAS (Network Access Servers) registered to the local RADIUS server.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show radius local-server nas [<ip-address>]
```

Parameter	Description
<ip-address>	Specify NAS IP address for show output.

Mode User Exec and Privileged Exec

Example The following command displays NAS information.

```
awplus# show radius local-server nas
```

Output

Table 11: Example output from the **show radius local-server nas** command

```
NAS-Address      Shared-Key

-----------------------------------------------------------

127.0.0.1       awplus-local-radius-server
```

Table 12: Parameters in the output of the **show radius local-server nas** command

Parameter	Description
NAS-Address	IP address of NAS.
Shared-Key	Shared key used for RADIUS connection.

Related Commands nas

show radius local-server statistics

Overview Use this command to display statistics about the local RADIUS server.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show radius local-server statistics
```

Mode User Exec and Privileged Exec

Usage Both unknown usernames and invalid passwords will display as failed logins in the show output.

Example The following command displays Local RADIUS server statistics.

```
awplus# show radius local-server statistics
```

Output

Table 13: Example output from the **show radius local-server statistics** command

```
Server status  : Run (administrative status is enable)
Enabled methods: MAC EAP-MD5 EAP-TLS EAP-PEAP

Successes :1 Unknown NAS :0
Failed Logins :0 Invalid packet from NAS :0
Internal Error :0 Unknown Error :0

NAS : 127.0.0.1
Successes :0 Shared key mismatch :0
Failed Logins :0 Unknown RADIUS message :0
Unknown EAP message :0 Unknown EAP auth type :0
Corrupted packet :0

NAS : 192.168.1.61
Successes :0 Shared key mismatch :0
Failed Logins :0 Unknown RADIUS message :0
Unknown EAP message :0 Unknown EAP auth type :0
Corrupted packet :0

Username  Successes  Failures
a 1 0
admin 0 0
```

Related Commands

clear radius local-server statistics

radius-server local

server enable

server auth-port

show radius local-server user

Overview Use this command to display information about the local RADIUS server user.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show radius local-server user [<user-name>]
show radius local-server user <user-name> format csv
```

Parameter	Description
`<user-name>`	RADIUS user name. If no user name is specified, information for all users is displayed.
`format`	File format.
`csv`	Comma separated value format.

Mode User Exec and Privileged Exec

Examples The following command displays Local RADIUS server user information for user Tom.

```
awplus# show radius local-server user Tom
```

Table 14: Example output from the **show radius local-server user** command

```
User-Name   Password   Group                Vlan
-----------------------------------------------------------------
Tom         abcd       NetworkOperators     ManagementNet
```

The following command displays all Local RADIUS server information for all users.

```
awplus# show radius local-server user
```

The following command displays Local RADIUS server user information for Tom in CSV format.

```
awplus# show radius local-server user Tom format csv
```

Table 15: Example output from the **show radius local-server user csv** command

```
true,"NetworkOperators","Tom",
"abcd",0,2099/01/
01,1,"","","ManagementNet",false,3600,false,0,"",false,"
```

Table 16: Parameters in the output from the **show radius local-server user** command

Parameter	Description
`User-Name`	User name.
`Password`	User password.
`Group`	Group name assigned to the user.
`Vlan`	VLAN name assigned to the user.

Related Commands

group

user (RADIUS server)

user (RADIUS server)

Overview Use this command to register a user to the local RADIUS server.

Use the **no** variant of this command to delete a user from the local RADIUS server.

Syntax

```
user <radius-user-name> [encrypted] password <user-password>
[group <user-group>]
```

```
no user <radius-user-name>
```

Parameter	Description
<radius-user-name>	RADIUS user name. This can also be a MAC address in the IEEE standard format of `HH-HH-HH-HH-HH-HH` if you are configuring MAC authentication to use local RADIUS server.
`encrypted`	Specifies that the password is being entered in its encrypted form, so that it is not further encrypted. When creating a new user, enter the password in plaintext, and do not use the **encrypted** parameter. Use the **encrypted** parameter only when referring to a user that has previously been created. For instance, when adding an existing user from another RADIUS server, use the **encrypted** parameter, and enter the encrypted version of the password that appears in the output of **show** commands for the user.
<user-password>	User password. This can also be a MAC address in the IEEE standard format of `HH-HH-HH-HH-HH-HH` if you are configuring MAC authentication to use local RADIUS server.
`group`	Specify the group for the user.
<user-group>	User group name.

Mode RADIUS Server Configuration

Usage RADIUS user names cannot contain question mark (`?`), space ( ), or quote (“ “) characters. RADIUS user names containing the below characters cannot use certificate authentication:

```
/ \ '$ &()*;< > '|
```

Certificates cannot be created and exported for RADIUS user names that contain the above characters. We advise you to avoid using these characters in RADIUS user names if you need to use certificate authentication, because you will not be able to create and export certificates.

You also can use the IEEE standard format hexadecimal notation (`HH-HH-HH-HH-HH-HH`) to specify a supplicant MAC address to configure the user name and user password parameters to use local RADIUS server for MAC Authentication. See the AAA Feature Overview and Configuration Guide for a sample MAC configuration. See also the command **user 00-db-59-ab-70-37 password 00-db-59-ab-70-37** as shown in the command examples.

Examples

The following commands add user `Tom` to the local RADIUS server and sets his password to `QwerSD`.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD
```

The following commands add user `Tom` to the local RADIUS server user group NormalUsers and sets his password `QwerSD`.

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user Tom password QwerSD group
NormalUsers
```

The following commands remove user Tom from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user Tom
```

The following commands add the supplicant MAC address 00-d0-59-ab-70-37 to the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# user 00-db-59-ab-70-37 password
00-db-59-ab-70-37
```

The following commands remove the supplicant MAC address 00-d0-59-ab-70-37 from the local RADIUS server:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# no user 00-db-59-ab-70-37
```

Related Commands

group

show radius local-server user

vlan (RADIUS server)

Overview Use this command to set the VLAN ID or name for the local RADIUS server user group. The VLAN information is used for authentication with the dynamic VLAN feature.

Use the **no** variant of this command to clear the VLAN ID or VLAN name for the local RADIUS server user group.

Syntax

```
vlan {<vid>|<vlan-name>}
no vlan
```

Parameter	Description
<vid>	VLAN ID.
<vlan-name>	VLAN name.

Default VLAN information is not set by default.

Mode RADIUS Server Group Configuration

Examples The following commands set VLAN ID 200 to the group named *NormalUsers*:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# vlan 200
```

The following commands remove VLAN ID 200 from the group named *NormalUsers*:

```
awplus# configure terminal
awplus(config)# radius-server local
awplus(config-radsrv)# group NormalUsers
awplus(config-radsrv-group)# no vlan
```

Related Commands group

show radius local-server user

34 TACACS+ Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure the device to use TACACS+ servers. For more information about TACACS+, see the TACACS+ Feature Overview and Configuration Guide.

Command List

show tacacs+

Overview This command displays the current TACACS+ server configuration and status.

Syntax

```
show tacacs+
```

Mode User Exec and Privileged Exec

Example To display the current status of TACACS+ servers, use the command:

```
awplus# show tacacs+
```

Output Figure 34-1: Example output from the **show tacacs+** command

```
TACACS+ Global Configuration
  Timeout              : 5 sec

Server Host/      Server
IP Address        Status
------------------------------------------------------------
192.168.1.10      Alive
192.168.1.11      Unknown
```

Table 1: Parameters in the output of the **show tacacs+** command

Output Parameter	Meaning	
`Timeout`	A time interval in seconds.	
`Server Host/IP Address`	TACACS+ server hostname or IP address.	
`Server Status`	The status of the authentication port.	
	`Alive`	The server is alive.
	`Dead`	The server has timed out.
	`Error`	The server is not responding or there is an error in the key string entered.
	`Unknown`	The server is never used or the status is unkown.
	`Unreachable`	The server is unreachable.
	`Unresolved`	The server name can not be resolved.

tacacs-server host

Overview Use this command to specify a remote TACACS+ server host for authentication, authorization and accounting, and to set the shared secret key to use with the TACACS+ server. The parameters specified with this command override the corresponding global parameters for TACACS+ servers.

Use the **no** variant of this command to remove the specified server host as a TACACS+ authentication and authorization server.

Syntax

```
tacacs-server host {<host-name>|<ip-address>} [key
[8]<key-string>]
```

```
no tacacs-server host {<host-name>|<ip-address>}
```

Parameter	Description
<host-name>	Server host name. The DNS name of the TACACS+ server host.
<ip-address>	The IP address of the TACACS+ server host, in dotted decimal notation A.B.C.D.
`key`	Set shared secret key with TACACS+ servers.
`8`	Specifies that you are entering a password as a string that has already been encrypted instead of entering a plain text password. The running config displays the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and the TACACS+ server. This key must match the encryption used on the TACACS+ server. This setting overrides the global setting of the tacacs-server key command. If no key value is specified, the global value is used.

Default No TACACS+ server is configured by default.

Mode Global Configuration

Usage A TACACS+ server host cannot be configured multiple times like a RADIUS server.

As many as four TACACS+ servers can be configured and consulted for login authentication, enable password authentication and accounting. The first server configured is regarded as the primary server and if the primary server fails then the backup servers are consulted in turn. A backup server is consulted if the primary server fails, not if a login authentication attempt is rejected. The reasons a server would fail are:

- it is not network reachable
- it is not currently TACACS+ capable

- it cannot communicate with the switch properly due to the switch and the server having different secret keys

Examples

To add the server `tac1.company.com` as the TACACS+ server host, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host tac1.company.com
```

To set the secret key to `secret` on the TACACS+ server `192.168.1.1`, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server host 192.168.1.1 key secret
```

To remove the TACACS+ server `tac1.company.com`, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server host tac1.company.com
```

Related Commands

aaa accounting commands

aaa authentication login

tacacs-server key

tacacs-server timeout

show tacacs+

tacacs-server key

Overview This command sets a global secret key for TACACS+ authentication, authorization and accounting. The shared secret text string is used for TACACS+ communications between the switch and all TACACS+ servers.

Note that if no secret key is explicitly specified for a TACACS+ server with the tacacs-server host command, the global secret key will be used for the shared secret for the server.

Use the **no** variant of this command to remove the global secret key.

Syntax

```
tacacs-server key [8] <key-string>
no tacacs-server key
```

Parameter	Description
8	Specifies a string in an encrypted format instead of plain text. The running config will display the new password as an encrypted string even if password encryption is turned off.
<key-string>	Shared key string applied, a value in the range 1 to 64 characters. Specifies the shared secret authentication or encryption key for all TACACS+ communications between this device and all TACACS+ servers. This key must match the encryption used on the TACACS+ server.

Mode Global Configuration

Usage Use this command to set the global secret key shared between this client and its TACACS+ servers. If no secret key is specified for a particular TACACS+ server using the tacacs-server host command, this global key is used.

Examples To set the global secret key to `secret` for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server key secret
```

To delete the global secret key for TACACS+ server, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server key
```

Related Commands tacacs-server host

show tacacs+

tacacs-server timeout

Overview Use this command to specify the TACACS+ global timeout value. The timeout value is how long the device waits for a reply to a TACACS+ request before considering the server to be dead.

Note that this command configures the **timeout** parameter for TACACS+ servers globally.

The **no** variant of this command resets the transmit timeout to the default (5 seconds).

Syntax

```
tacacs-server timeout <seconds>
no tacacs-server timeout
```

Parameter	Description
<seconds>	TACACS+ server timeout in seconds, in the range 1 to 1000.

Default The default timeout value is 5 seconds.

Mode Global Configuration

Examples To set the timeout value to 3 seconds, use the following commands:

```
awplus# configure terminal
awplus(config)# tacacs-server timeout 3
```

To reset the timeout period for TACACS+ servers to the default, use the following commands:

```
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

Related Commands tacacs-server host

show tacacs+

35 DHCP Snooping Commands

Introduction

Overview

This chapter gives detailed information about the commands used to configure DHCP snooping. For detailed descriptions of related ACL commands, see IPv4 Hardware Access Control List (ACL) Commands. For more information about DHCP snooping, see the DHCP Snooping Feature Overview and Configuration Guide.

DHCP snooping can operate on static link aggregators (e.g. sa2) and dynamic link aggregators (e.g. po2), as well as on switch ports (e.g. port1.0.2).

Command List

arp security

Overview Use this command to enable ARP security on untrusted ports in the VLANs, so that the switch only responds to/forwards ARP packets if they have recognized IP and MAC source addresses.

Use the **no** variant of this command to disable ARP security on the VLANs.

Syntax

```
arp security
no arp security
```

Default Disabled

Mode Interface Configuration (VLANs)

Usage Enable ARP security to provide protection against ARP spoofing. DHCP snooping must also be enabled on the switch (service dhcp-snooping command), and on the VLANs (ip dhcp snooping command).

Example To enable ARP security on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# arp security
```

Related Commands

arp security violation

show arp security

show arp security interface

show arp security statistics

arp security violation

Overview Use this command to specify an additional action to perform if an ARP security violation is detected on the ports. ARP security must also be enabled (arp security command).

Use the **no** variant of this command to remove the specified action, or all actions. Traffic violating ARP security will be dropped, but no other action will be taken.

Syntax

```
arp security violation {log|trap|link-down} ...
no arp security violation [log|trap|link-down] ...
```

Parameter	Description
`log`	Generate a log message. To display these messages, use the show log command.
`trap`	Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the snmp-server enable trap command. Notifications are limited to one per second and to one per source MAC and violation reason. Additional violations within a second of a notification being sent will not result in further notifications. Default: disabled.
`link-down`	Shut down the port that received the packet. Default: disabled.

Default When the switch detects an ARP security violation, it drops the packet. By default, it does not perform any other violation actions.

Mode Interface Configuration (switch ports, static or dynamic aggregated links)

Usage When the switch detects an ARP security violation on an untrusted port in a VLAN that has ARP security enabled, it drops the packet. This command sets the switch to perform additional actions in response to ARP violations.

If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the shutdown command.

Example To send SNMP notifications for ARP security violations on ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# arp security violation trap
```

Related Commands

arp security

show arp security interface

show arp security statistics

show log

snmp-server enable trap

clear arp security statistics

Overview Use this command to clear ARP security statistics for the specified ports, or for all ports.

Syntax

```
clear arp security statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The ports may be switch ports, or static or dynamic link aggregators.

Mode Privileged Exec

Example To clear statistics for ARP security on interface port1.0.1, use the command:

```
awplus# clear arp security statistics interface port1.0.1
```

Related Commands

arp security violation

show arp security

show arp security statistics

clear ip dhcp snooping binding

Overview Use this command to remove one or more DHCP Snooping dynamic entries from the DHCP Snooping binding database. If no options are specified, all entries are removed from the database.

CAUTION: If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.

Syntax

```
clear ip dhcp snooping binding [<ipaddr>] [interface
<port-list>] [vlan <vid-list>]
```

Parameter	Description
<ipaddr>	Remove the entry for this client IP address.
<port-list>	Remove all entries for these ports. The port list may contain switch ports, and static or dynamic link aggregators (channel groups).
<vid-list>	Remove all entries associated with these VLANs.

Mode Privileged Exec

Usage This command removes dynamic entries from the database. Note that dynamic entries can also be deleted by using the **no** variant of the ip dhcp snooping binding command.

Dynamic entries can individually restored by using the ip dhcp snooping binding command.

To remove static entries, use the **no** variant of the ip source binding command.

Example To remove a dynamic lease entry from the DHCP snooping database for a client with the IP address 192.168.1.2, use the command:

```
awplus# clear ip dhcp snooping binding 192.168.1.2
```

Related Commands

ip dhcp snooping binding

ip source binding

show ip dhcp snooping binding

clear ip dhcp snooping statistics

Overview Use this command to clear DHCP snooping statistics for the specified ports, or for all ports.

Syntax

```
clear ip dhcp snooping statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports to clear statistics for. If no ports are specified, statistics are cleared for all ports. The port list can contain switch ports, or static or dynamic link aggregators.

Mode Privileged Exec

Example To clear statistics for the DHCP snooping on interface port1.0.1, use the command:

```
awplus# clear ip dhcp snooping statistics interface port1.0.1
```

Related Commands

clear arp security statistics

show ip dhcp snooping

show ip dhcp snooping statistics

debug arp security

Overview Use this command to enable ARP security debugging.

Use the **no** variant of this command to disable debugging for ARP security.

Syntax

```
debug arp security
no debug arp security
```

Default Disabled

Mode Privileged Exec

Example To enable ARP security debugging, use the commands:

```
awplus# debug arp security
```

Related Commands

show debugging arp security

show log

terminal monitor

debug ip dhcp snooping

Overview Use this command to enable the specified types of debugging for DHCP snooping.

Use the **no** variant of this command to disable the specified types of debugging.

Syntax

```
debug ip dhcp snooping {all|acl|db|packet [detail]}
no debug ip dhcp snooping {all|acl|db|packet [detail]}
```

Parameter	Description
`all`	All DHCP snooping debug.
`acl`	DHCP snooping access list debug.
`db`	DHCP snooping binding database debug.
`packet`	DHCP snooping packet debug. For the **no** variant of this command, this option also disables detailed packet debug, if it was enabled.
`detail`	Detailed packet debug.

Default Disabled

Mode Privileged Exec

Example To enable access list debugging for DHCP snooping, use the commands:

```
awplus# debug ip dhcp snooping acl
```

Related Commands

debug arp security

show debugging ip dhcp snooping

show log

terminal monitor

ip dhcp snooping

Overview Use this command to enable DHCP snooping on one or more VLANs.

Use the **no** variant of this command to disable DHCP snooping on the VLANs.

Syntax

```
ip dhcp snooping
no ip dhcp snooping
```

Default DHCP snooping is disabled on VLANs by default.

Mode Interface Configuration (VLANs)

Usage For DHCP snooping to operate on a VLAN, it must:

- be enabled on the particular VLAN by using this command
- be enabled globally on the switch by using the service dhcp-snooping command
- have at least one port connected to a DHCP server configured as a trusted port by using the ip dhcp snooping trust command

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on particular VLANs using this command, you must also remove any DHCP snooping ACLs from the ports to maintain connectivity (no access-group command).

Examples To enable DHCP snooping on VLANs 2 to 4, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# ip dhcp snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# interface vlan2-vlan4
awplus(config-if)# no ip dhcp snooping
```

Related Commands

ip dhcp snooping trust

service dhcp-snooping

show ip dhcp snooping

ip dhcp snooping agent-option

Overview Use this command to enable DHCP Relay Agent Option 82 information insertion on the switch. When this is enabled, the switch:

- inserts DHCP Relay Agent Option 82 information into DHCP packets that it receives on untrusted ports
- removes DHCP Relay Agent Option 82 information from DHCP packets that it sends to untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 insertion.

Syntax

```
ip dhcp snooping agent-option
no ip dhcp snooping agent-option
```

Default DHCP Relay Agent Option 82 insertion is enabled by default when DHCP snooping is enabled.

Mode Global Configuration

Usage DHCP snooping must also be enabled on the switch (service dhcp-snooping command), and on the VLANs (ip dhcp snooping command).

If a subscriber ID is configured for the port (ip dhcp snooping subscriber-id command), the switch includes this in the DHCP Relay Agent Option 82 information it inserts into DHCP packets received on the port.

Example To disable DHCP Relay Agent Option 82 on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping agent-option
```

Related Commands

ip dhcp snooping

ip dhcp snooping agent-option allow-untrusted

ip dhcp snooping subscriber-id

service dhcp-snooping

show ip dhcp snooping

ip dhcp snooping agent-option allow-untrusted

Overview Use this command to enable DHCP Relay Agent Option 82 information reception on untrusted ports. When this is enabled, the switch accepts incoming DHCP packets that contain DHCP Relay Agent Option 82 information on untrusted ports.

Use the **no** variant of this command to disable DHCP Relay Agent Option 82 information reception on untrusted ports.

Syntax

```
ip dhcp snooping agent-option allow-untrusted
no ip dhcp snooping agent-option allow-untrusted
```

Default Disabled

Mode Global Configuration

Usage If the switch is connected via untrusted ports to edge switches that insert DHCP Relay Agent Option 82 information into DHCP packets, you may need to allow these DHCP packets through the untrusted ports, by using this command.

When this is disabled (default), the switch treats incoming DHCP packets on untrusted ports that contain DHCP Relay Agent Option 82 information as DHCP snooping violations: it drops them and applies any violation action specified by the ip dhcp snooping violation command. The switch stores statistics for packets dropped; to display these statistics, use the show ip dhcp snooping statistics command.

Example To enable DHCP snooping Option 82 information reception on untrusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping agent-option allow-untrusted
```

Related Commands

ip dhcp snooping agent-option

ip dhcp snooping violation

show ip dhcp snooping

show ip dhcp snooping statistics

ip dhcp snooping agent-option circuit-id vlantriplet

Overview Use this command to specify the Circuit ID sub-option of the DHCP Relay Agent Option 82 field as the VLAN ID and port number. The Circuit ID specifies the switch port and VLAN ID that the client-originated DHCP packet was received on.

Use the **no** variant of this command to set the Circuit ID to the default, the VLAN ID and Ifindex (interface number).

Syntax

```
ip dhcp snooping agent-option circuit-id vlantriplet
no ip dhcp snooping agent-option circuit-id
```

Default By default, the Circuit ID is the VLAN ID and Ifindex (interface number).

Mode Interface Configuration for a VLAN interface.

Usage The Circuit ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled (ip dhcp snooping agent-option command; enabled by default), and
- DHCP snooping is enabled on the switch (service dhcp-snooping) and on the VLAN to which the port belongs (ip dhcp snooping)

Examples To set the Circuit ID to `vlantriplet` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option circuit-id
vlantriplet
```

To return the Circuit ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option circuit-id
```

Related Commands

ip dhcp snooping agent-option

ip dhcp snooping agent-option remote-id

show ip dhcp snooping

show ip dhcp snooping agent-option

ip dhcp snooping agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field. The Remote ID identifies the device that inserted the Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the switch's MAC address.

Use the **no** variant of this command to set the Remote ID to the default, the switch's MAC address.

Syntax

```
ip dhcp snooping agent-option remote-id <remote-id>
no ip dhcp snooping agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. If the Remote ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Default The Remote ID is set to the switch's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of forwarded client DHCP packets:

- DHCP snooping Option 82 information insertion is enabled (ip dhcp snooping agent-option command; enabled by default), and
- DHCP snooping is enabled on the switch (service dhcp-snooping) and on the VLAN to which the port belongs (ip dhcp snooping)

Examples To set the Remote ID to `myid` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp snooping agent-option remote-id myid
```

To return the Remote ID format to the default for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp snooping agent-option remote-id
```

Related Commands

ip dhcp snooping agent-option

ip dhcp snooping agent-option circuit-id vlantriplet

show ip dhcp snooping

show ip dhcp snooping agent-option

ip dhcp snooping binding

Overview Use this command to manually add a dynamic-like entry (with an expiry time) to the DHCP snooping database. Once added to the database, this entry is treated as a dynamic entry, and is stored in the DHCP snooping database backup file. This command is not stored in the switch's running configuration.

Use the **no** variant of this command to delete a dynamic entry for an IP address from the DHCP snooping database, or to delete all dynamic entries from the database.

CAUTION: If you remove entries from the database for current clients, they will lose IP connectivity until they request and receive a new DHCP lease. If you clear all entries, all clients connected to untrusted ports will lose connectivity.

Syntax

```
ip dhcp snooping binding <ipaddr> [<macaddr>] vlan <vid>
interface <port> expiry <expiry-time>
```

```
no ip dhcp snooping binding [<ipaddr>]
```

Parameter	Description
<ipaddr>	Client's IP address.
<macaddr>	Client's MAC address in HHHH.HHHH.HHHH format.
<vid>	The VLAN ID for the entry, in the range 1 to 4094.
<port>	The port the client is connected to. The port can be a switch port, or a static or dynamic link aggregation (channel group).
<expiry-time>	The expiry time for the entry, in the range 5 to 2147483647 seconds.

Mode Privileged Exec

Usage Note that dynamic entries can also be deleted from the DHCP snooping database by using the clear ip dhcp snooping binding command.

To add or remove static entries from the database, use the ip source binding command.

Example To restore an entry in the DHCP snooping database for a DHCP client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, and with an expiry time of 1 hour, use the commands:

```
awplus# ip dhcp snooping binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6 expiry 3600
```

Related Commands

clear ip dhcp snooping binding

ip source binding

show ip dhcp snooping binding

ip dhcp snooping database

Overview Use this command to set the location of the file to which the dynamic entries in the DHCP snooping database are written. This file provides a backup for the DHCP snooping database.

Use the **no** variant of this command to set the database location back to the default, **nvs**.

Syntax

```
ip dhcp snooping database {nvs|flash|usb}
no ip dhcp snooping database
```

Parameter	Description
`nvs`	The switch checks the database and writes the file to non-volatile storage (NVS) on the switch at 2 second intervals if it has changed.
`flash`	The switch checks the database and writes the file to Flash memory on the switch at 60 second intervals if it has changed.
`usb`	The switch checks the database and writes the file to a USB storage device installed in the switch at 2 second intervals if it has changed.

Default NVS

Mode Global Configuration

Usage In a stack, the backup file is automatically synchronized across all stack members to the location configured. If the backup file is stored on a USB storage device on the stack master, it is only synchronized across stack members that also have USB storage devices installed.

If the location of the backup file is changed by using this command, a new file is created in the new location, and the old version of the file remains in the old location. This can be removed if necessary (hidden file: **.dhcp.dsn.gz**).

Example To set the location of the DHCP snooping database to non-volatile storage on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping database nvs
```

Related Commands show ip dhcp snooping

ip dhcp snooping delete-by-client

Overview Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when it receives a valid DHCP release message with matching IP address, VLAN ID, and client hardware address on an untrusted port, and to discard release messages that do not match an entry in the database.

Use the **no** variant of this command to set the switch to forward DHCP release messages received on untrusted ports without removing any entries from the database.

Syntax

```
ip dhcp snooping delete-by-client
no ip dhcp snooping delete-by-client
```

Default Enabled: by default, DHCP lease entries are deleted from the DHCP snooping database when matching DHCP release messages are received.

Mode Global Configuration

Usage DHCP clients send a release message when they no longer wish to use the IP address they have been allocated by a DHCP server. Use this command to enable DHCP snooping to use the information in these messages to remove entries from its database immediately. Use the **no** variant of this command to ignore these release messages. Lease entries corresponding to ignored DHCP release messages eventually time out when the lease expires.

Examples To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when a matching release message is received, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-client
```

To set the switch to forward and ignore the content of any DHCP release messages it receives, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-client
```

Related Commands show ip dhcp snooping

ip dhcp snooping delete-by-linkdown

Overview Use this command to set the switch to remove a dynamic entry from the DHCP snooping database when its port goes down. If the port is part of an aggregated link, the entries in the database are only deleted if all the ports in the aggregated link are down.

Use the **no** variant of this command to set the switch not to delete entries when ports go down.

Syntax

```
ip dhcp snooping delete-by-linkdown
no ip dhcp snooping delete-by-linkdown
```

Default Disabled: by default DHCP Snooping bindings are not deleted when an interface goes down.

Mode Global Configuration

Usage If this command is enabled in a stack, and the master goes down and is replaced by a new master, entries in the DHCP snooping database for ports on the master are removed, unless they are part of link aggregators that are still up.

Examples To set the switch to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp snooping delete-by-linkdown
```

To set the switch not to delete DHCP snooping lease entries from the DHCP snooping database when links go down, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping delete-by-linkdown
```

Related Commands show ip dhcp snooping

ip dhcp snooping max-bindings

Overview Use this command to set the maximum number of DHCP lease entries that can be stored in the DHCP snooping database for each of the ports. Once this limit has been reached, no further DHCP lease allocations made to devices on the port are stored in the database.

Use the **no** variant of this command to reset the maximum to the default, 1.

Syntax

```
ip dhcp snooping max-bindings <0-520>
no ip dhcp snooping max-bindings
```

Parameter	Description
<0-520>	The maximum number of bindings that will be stored for the port in the DHCP snooping binding database. If 0 is specified, no entries will be stored in the database for the port.

Default The default for maximum bindings is 1.

Mode Interface Configuration (port)

Usage The maximum number of leases cannot be changed for a port while there are DHCP snooping Access Control Lists (ACL) associated with the port. Before using this command, remove any DHCP snooping ACLs associated with the ports. To display ACLs used for DHCP snooping, use the show ip dhcp snooping acl command.

In general, the default (1) will work well on an edge port with a single directly connected DHCP client. If the port is on an aggregation switch that is connected to an edge switch with multiple DHCP clients connected through it, then use this command to increase the number of lease entries for the port.

If there are multiple VLANs configured on the port, the limit is shared between all the VLANs on this port. For example, the default only allows one lease to be stored for one VLAN. To allow connectivity for the other VLANs, use this command to increase the number of lease entries for the port.

Example To set the maximum number of bindings to be stored in the DHCP snooping database to 10 per port for ports 1.0.1 to 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.6
awplus(config-if)# ip dhcp snooping max-bindings 10
```

Related Commands

access-group

show ip dhcp snooping acl

show ip dhcp snooping interface

ip dhcp snooping subscriber-id

Overview Use this command to set a Subscriber ID for the ports.

Use the **no** variant of this command to remove Subscriber IDs from the ports.

Syntax

```
ip dhcp snooping subscriber-id [<sub-id>]
no ip dhcp snooping subscriber-id
```

Parameter	Description
<sub-id>	The Subscriber ID; an alphanumeric (ASCII) string 1 to 50 characters in length. If the Subscriber ID contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Default No Subscriber ID.

Mode Interface Configuration (port)

Usage The Subscriber ID sub-option is included in the DHCP Relay Agent Option 82 field of client DHCP packets forwarded from a port if:

- a Subscriber ID is specified for the port using this command, and
- DHCP snooping Option 82 information insertion is enabled (ip dhcp snooping agent-option command; enabled by default), and
- DHCP snooping is enabled on the switch (service dhcp-snooping) and on the VLAN to which the port belongs (ip dhcp snooping)

Examples To set the Subscriber ID for port 1.0.3 to **room_534**, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# ip dhcp snooping subscriber-id room_534
```

To remove the Subscriber ID from port 1.0.3, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# no ip dhcp snooping subscriber-id
```

Related Commands ip dhcp snooping agent-option

show ip dhcp snooping interface

ip dhcp snooping trust

Overview Use this command to set the ports to be DHCP snooping trusted ports.

Use the **no** variant of this command to return the ports to their default as untrusted ports.

Syntax

```
ip dhcp snooping trust
no ip dhcp snooping trust
```

Default All ports are untrusted by default.

Mode Interface Configuration (port)

Usage Typically, ports connecting the switch to trusted elements in the network (towards the core) are set as trusted ports, while ports connecting untrusted network elements are set as untrusted. Configure ports connected to DHCP servers as trusted ports.

Example To set switch ports 1.0.1 and 1.0.2 to be trusted ports, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1-port1.0.2
awplus(config-if)# ip dhcp snooping trust
```

Related Commands show ip dhcp snooping interface

ip dhcp snooping verify mac-address

Overview Use this command to verify that the source MAC address and client hardware address match in DHCP packets received on untrusted ports.

Use the **no** variant of this command to disable MAC address verification.

Syntax

```
ip dhcp snooping verify mac-address
no ip dhcp snooping verify mac-address
```

Default Enabled—source MAC addresses are verified by default.

Mode Global Configuration

Usage When MAC address verification is enabled, the switch treats DHCP packets with source MAC address and client hardware address that do not match as DHCP snooping violations: it drops them and applies any other violation action specified by the ip dhcp snooping violation command. To bring the port back up again after any issues have been resolved, use the shutdown command.

Example To disable MAC address verification on the switch, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp snooping verify mac-address
```

Related Commands

ip dhcp snooping violation

show ip dhcp snooping

show ip dhcp snooping statistics

ip dhcp snooping violation

Overview Use this command to specify the action the switch will take when it detects a DHCP snooping violation by a DHCP packet on the ports.

Use the **no** variant of this command to disable the specified violation actions, or all violation actions.

Syntax

```
ip dhcp snooping violation {log|trap|link-down} ...
no ip dhcp snooping violation [{log|trap|link-down} ...]
```

Parameter	Description
`log`	Generate a log message. To display these messages, use the show log command. Default: disabled.
`trap`	Generate an SNMP notification (trap). To send SNMP notifications, SNMP must also be configured, and DHCP snooping notifications must be enabled using the snmp-server enable trap command. Notifications are limited to one per second and to one per source MAC and violation reason. Default: disabled.
`link-down`	Set the port status to link-down. Default: disabled.

Default By default, DHCP packets that violate DHCP snooping are dropped, but no other violation action is taken.

Mode Interface Configuration (port)

Usage If a port has been shut down in response to a violation, to bring it back up again after any issues have been resolved, use the shutdown command.

IP packets dropped by DHCP snooping filters do not result in other DHCP snooping violation actions.

Example To set the switch to send an SNMP notification and set the link status to link-down if it detects a DHCP snooping violation on switch ports 1.0.1 to 1.0.4, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap dhcpsnooping
awplus(config)# interface port1.0.1-port1.0.4
awplus(config-if)# ip dhcp snooping violation trap link-down
```

Related Commands

show ip dhcp snooping interface

show log

snmp-server enable trap

ip source binding

Overview Use this command to add or replace a static entry in the DHCP snooping database.

Use the **no** variant of this command to delete the specified static entry or all static entries from the database.

Syntax

```
ip source binding <ipaddr> [<macaddr>] vlan <vid> interface
<port>
```

```
no ip source binding [<ipaddr>]
```

Parameter	Description
<ipaddr>	Client's IP address. If there is already an entry in the DHCP snooping database for this IP address, then this command replaces it with the new entry.
<macaddr>	Client's MAC address in HHHH.HHHH.HHHH format.
<vid>	The VLAN ID associated with the entry.
<port>	The port the client is connected to.

Mode Global Configuration

Usage This command removes static entries from the database.

To remove dynamic entries, use the clear ip dhcp snooping binding command or the **no** variant of the ip dhcp snooping binding command.

Examples To add a static entry to the DHCP snooping database for a client with the IP address 192.168.1.2, MAC address 0001.0002.0003, on port1.0.6 of vlan6, use the command:

```
awplus# configure terminal
```

```
awplus(config)# ip source binding 192.168.1.2 0001.0002.0003
vlan 6 interface port1.0.6
```

To remove the static entry for IP address 192.168.1.2 from the database, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ip source binding 192.168.1.2
```

To remove all static entries from the database, use the commands:

```
awplus# configure terminal
```

```
awplus(config)# no ip source binding
```

Related Commands

clear ip dhcp snooping binding

ip dhcp snooping binding

show ip dhcp snooping binding

show ip source binding

service dhcp-snooping

Overview Use this command to enable the DHCP snooping service globally on the switch. This must be enabled before other DHCP snooping configuration commands can be entered.

Use the **no** variant of this command to disable the DHCP snooping service on the switch. This removes all DHCP snooping configuration from the running configuration, except for any DHCP snooping maximum bindings settings (ip dhcp snooping max-bindings command), and any DHCP snooping-based Access Control Lists (ACLs), which are retained when the service is disabled.

Syntax

```
service dhcp-snooping
no service dhcp-snooping
```

Default DHCP snooping is disabled on the switch by default.

Mode Global Configuration

Usage For DHCP snooping to operate on a VLAN, it must be enabled on the switch by using this command, and also enabled on the particular VLAN by using the ip dhcp snooping command.

For DHCP snooping to operate on a VLAN, it must:

- be enabled globally on the switch by using this command
- be enabled on the particular VLAN by using the ip dhcp snooping command
- have at least one port connected to a DHCP server configured as a trusted port by using the ip dhcp snooping trust command

If you disable the DHCP snooping service by using the **no** variant of this command, all DHCP snooping configuration (including ARP security, but excluding maximum bindings and ACLs) is removed from the running configuration, and the DHCP snooping database is deleted from active memory. If you re-enable the service, the switch repopulates the DHCP snooping database from the dynamic lease entries in the database backup file (in NVS by default—see the ip dhcp snooping database command). The lease expiry times are updated.

The DHCP snooping service cannot be enabled on a switch that is configured with any of the following features, or vice versa:

- web authentication (auth-web enable command)
- roaming authentication (auth roaming enable command, auth roaming disconnected command)
- guest VLAN authentication (auth guest-vlan command).
- DHCP relay agent option (ip dhcp-relay agent-option command)

Any ACLs on a port that permit traffic matching DHCP snooping entries and block other traffic, will block all traffic if DHCP snooping is disabled on the port. If you disable DHCP snooping on the switch using this command, you must also remove

any DHCP snooping ACLs from the ports to maintain connectivity (no access-group command).

Examples

To enable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# service dhcp-snooping
```

To disable DHCP snooping on the switch, use the command:

```
awplus# configure terminal
awplus(config)# no service dhcp-snooping
```

Related Commands

ip dhcp snooping

ip dhcp snooping database

ip dhcp snooping max-bindings

show ip dhcp snooping

show arp security

Overview Use this command to display ARP security configuration.

Syntax

```
show arp security
```

Mode User Exec and Privileged Exec

Example To display ARP security configuration on the switch use the command:

```
awplus# show arp security
```

Table 1: Example output from the **show arp security** command

```
awplus# show arp security

ARP Security Information:
  Total VLANs enabled ..... 2
  Total VLANs disabled ..... 11
  vlan1 ..... Disabled
  vlan2 ..... Disabled
  vlan3 ..... Disabled
  vlan4 ..... Disabled
  vlan5 ..... Disabled
  vlan100 ..... Disabled
  vlan101 ..... Disabled
  vlan102 ..... Disabled
  vlan103 ..... Disabled
  vlan104 ..... Disabled
  vlan105 ..... Enabled
  vlan1000 ..... Disabled
  vlan1001 ..... Enabled
```

Table 2: Parameters in the output from the **show arp security** command

Parameter	Description
`Total VLANs enabled`	The number of VLANs that have ARP security enabled.
`Total VLANs disabled`	The number of VLANs that have ARP security disabled.

Related Commands

arp security

show arp security interface

show arp security statistics

show arp security interface

Overview Use this command to display ARP security configuration for the specified ports or all ports.

Syntax `show arp security interface [<port-list>]`

Parameter	Description
<port-list>	The ports to display ARP security information about. The port list can include switch ports, and static or dynamic aggregated links.

Mode User Exec and Privileged Exec

Example To display ARP security configuration for ports, use the command:

```
awplus# show arp security interface
```

Table 3: Example output from the **show arp security interface** command

```
awplus#show arp security interface

Arp Security Port Status and Configuration:

  Port: Provisioned ports marked with brackets, e.g. (portx.y.z)
  KEY:  LG = Log
        TR = Trap
        LD = Link down

Port         Action
------------------------------
port1.0.1    -- -- --
port1.0.2    -- -- --
port1.0.3    LG TR LD
port1.0.4    LG -- --
port1.0.5    LG -- --
port1.0.6    LG TR --
port1.0.7    LG -- LD
...
```

Table 4: Parameters in the output from the **show arp security interface** command

Parameter	Description
`Action`	The action the switch takes when it detects an ARP security violation on the port.
`Port`	The port. Parentheses indicate that ports are configured for provisioning.
`LG, Log`	Generate a log message
`TR, Trap`	Generate an SNMP notification (trap).
`LD, Link down`	Shut down the link.

Related Commands

arp security violation

show arp security

show arp security statistics

show log

snmp-server enable trap

show arp security statistics

Overview Use this command to display ARP security statistics for the specified ports or all ports.

Syntax `show arp security statistics [detail] [interface <port-list>]`

Parameter	Description
`detail`	Display detailed statistics.
`interface <port-list>`	Display statistics for the specified ports.

Mode User Exec and Privileged Exec

Example To display the brief statistics for the ARP security, use the command:

```
awplus# show arp security statistics
```

Table 5: Example output from the **show arp security statistics** command

```
awplus# show arp security statistics

DHCP Snooping ARP Security Statistics:
              In          In
 Interface    Packets     Discards
---------------------------------
 port1.0.3    20          20
 port1.0.4    30          30
 port1.0.12   120         0
```

Table 6: Parameters in the output from the **show arp security statistics** command

Parameter	Description
`Interface`	A port name. Parentheses indicate that ports are configured for provisioning.
`In Packets`	The total number of incoming ARP packets that are processed by DHCP Snooping ARP Security
`In Discards`	The total number of ARP packets that are dropped by DHCP Snooping ARP Security.

Table 7: Example output from the **show arp security statistics detail** command

```
awplus#show arp security statistics detail

DHCP Snooping ARP Security Statistics:
Interface ..................... port1.0.3
  In Packets .................. 20
  In Discards ................. 20
    No Lease .................. 20
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
Interface ..................... port1.0.4
  In Packets .................. 30
  In Discards ................. 30
    No Lease .................. 30
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
Interface ..................... port1.0.12
  In Packets .................. 120
  In Discards ................. 0
    No Lease .................. 0
    Bad Vlan .................. 0
    Bad Port .................. 0
    Source Ip Not Allocated .... 0
```

Related Commands

arp security

arp security violation

clear arp security statistics

show arp security

show arp security interface

show log

show debugging arp security

Overview Use this command to display the ARP security debugging configuration.

Syntax

```
show debugging arp security
```

Mode User and Privileged Exec

Example To display the debugging settings for ARP security on the switch, use the command:

```
awplus# show debugging arp security
```

Table 8: Example output from the **show debugging arp security** command

```
awplus# show debugging arp security

ARP Security debugging status:
  ARP Security debugging is off
```

Related Commands

arp security violation

debug arp security

show debugging ip dhcp snooping

Overview Use this command to display the DHCP snooping debugging configuration.

Syntax

```
show debugging ip dhcp snooping
```

Mode User Exec and Privileged Exec

Example To display the DHCP snooping debugging configuration, use the command:

```
awplus# show debugging ip dhcp snooping
```

Table 9: Example output from the **show debugging ip dhcp snooping** command

```
awplus# show debugging ip dhcp snooping

DHCP snooping debugging status:
  DHCP snooping debugging is off
  DHCP snooping all debugging is off
  DHCP snooping acl debugging is off
  DHCP snooping binding DB debugging is off
  DHCP snooping packet debugging is off
  DHCP snooping detailed packet debugging is off
```

Related Commands

debug ip dhcp snooping

show log

show ip dhcp snooping

Overview Use this command to display DHCP snooping global configuration on the switch.

Syntax

```
show ip dhcp snooping
```

Mode User Exec and Privileged Exec

Example To display global DHCP snooping configuration on the switch, use the command:

```
awplus# show ip dhcp snooping
```

Table 10: Example output from the **show ip dhcp snooping** command

```
DHCP Snooping Information:
  DHCP Snooping service ............. Enabled

Option 82 insertion ............... Enabled

Option 82 on untrusted ports ...... Not allowed
  Binding delete by client .......... Disabled
  Binding delete by link down ....... Disabled
  Verify MAC address ................ Disabled
  SNMP DHCP Snooping trap ........... Disabled

DHCP Snooping database:
  Database location ................. nvs  Number of entries in
database ..... 2

DHCP Snooping VLANs:
  Total VLANs enabled ............... 1
  Total VLANs disabled .............. 9
  vlan1 ............... Enabled
  vlan2 ............... Disabled
  vlan3 ............... Disabled
  vlan4 ............... Disabled
  vlan5 ............... Disabled
  vlan100 ............. Disabled
  vlan101 ............. Disabled
  vlan105 ............. Disabled
  vlan1000 ............ Disabled
  vlan1001 ............ Disabled
```

Related Commands

service dhcp-snooping

show arp security

show ip dhcp snooping acl

show ip dhcp snooping agent-option

show ip dhcp snooping binding

show ip dhcp snooping interface

show ip dhcp snooping acl

Overview Use this command to display information about the Access Control Lists (ACL) that are using the DHCP snooping database.

Syntax

```
show ip dhcp snooping acl
show ip dhcp snooping acl [detail|hardware] [interface
[<interface-list>]]
```

Parameter	Description
`detail`	Detailed DHCP Snooping ACL information.
`hardware`	DHCP Snooping hardware ACL information.
`interface`	ACL Interface information.
<interface-list>	The interfaces to display information about.

Mode User Exec and Privileged Exec

Example To display DHCP snooping ACL information, use the command:

```
awplus# show ip dhcp snooping acl
```

Table 11: Example output from the **show ip dhcp snooping acl** command

```
awplus#show ip dhcp snooping acl

DHCP Snooping Based Filters Summary:

                       Maximum   Template  Attached
Interface    Bindings  Bindings  Filters   Hardware Filters
-------------------------------------------------------------
 port1.0.1   1         520       0         0
 port1.0.2   1         3         2         6
 port1.0.3   1         2         4         8
 port1.0.4   1         2         7         14
 port1.0.5   0         2         6         12
 port1.0.6   0         1         0         0
 port1.0.7   0         1         0         0
 port1.0.8   0         1         0         0
 port1.0.9   0         1         0         0
 port1.0.10  0         1         0         0
 port1.0.11  0         1         0         0
 port1.0.12  0         1         0         0
(port2.0.1 ) 0         520       0         0
(port2.0.2 ) 0         1         0         0
```

To display DHCP snooping hardware ACL information, use the command:

```
awplus# show ip dhcp snooping acl hardware
```

Table 12: Example output from the **show ip dhcp snooping acl hardware** command

```
awplus#show ip dhcp snooping acl hardware

DHCP Snooping Based Filters in Hardware:

Interface    Access-list(/ClassMap)        Source IP         Source MAC
-------------------------------------------------------------------------
 port1.0.2   dhcpsn1                       10.10.10.10       aaaa.bbbb.cccc
 port1.0.2   dhcpsn1                       20.20.20.20       0000.aaaa.bbbb
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.2   dhcpsn1                       0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 30.30.30.30       aaaa.bbbb.dddd
 port1.0.3   dhcpsn2/cmap1                 40.40.40.40       0000.aaaa.cccc
 port1.0.3   dhcpsn2/cmap1                 50.50.50.50       0000.aaaa.dddd
 port1.0.3   dhcpsn2/cmap1                 60.60.60.60       0000.aaaa.eeee
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.3   dhcpsn2/cmap1                 0.0.0.0           0000.0000.0000
 port1.0.4   dhcpsn3/cmap2                 70.70.70.70
 port1.0.4   dhcpsn3/cmap2                 80.80.80.80
 port1.0.4   dhcpsn2/cmap1                 70.70.70.70
 port1.0.4   dhcpsn2/cmap1                 80.80.80.80
 port1.0.4   dhcpsn1                       70.70.70.70
 port1.0.4   dhcpsn1                       80.80.80.80
```

To display detailed DHCP snooping ACL information for port 1.0.4, use the command:

```
awplus# show ip dhcp snooping acl detail interface port1.0.4
```

Table 13: Example output from the **show ip dhcp snooping acl detail interface** command

```
awplus#show ip dhcp snooping acl detail interface port1.0.4

DHCP Snooping Based Filters Information:

 port1.0.4 : Maximum Bindings ........... 2
 port1.0.4 : Template filters ........... 7
 port1.0.4 : Attached hardware filters .. 14
 port1.0.4 : Current bindings ........... 1, 1 free
 port1.0.4    Client 1 ................. 120.120.120.120
 port1.0.4 : Templates: cheese (via class-map: cmap2)
 port1.0.4 :  10 permit ip dhcpsnooping 100.0.0.0/8
 port1.0.4 : Template: dhcpsn2 (via class-map: cmap1)
 port1.0.4 :  10 permit ip dhcpsnooping any
 port1.0.4 :  20 permit ip dhcpsnooping 10.0.0.0/8
 port1.0.4 :  30 permit ip dhcpsnooping 20.0.0.0/8
 port1.0.4 :  40 permit ip dhcpsnooping 30.0.0.0/8
 port1.0.4 : Template: dhcpsn1 (via access-group)
 port1.0.4 :  10 permit ip dhcpsnooping any mac dhcpsnooping abcd.0000.0000 00
 00.ffff.ffff
 port1.0.4 : 20 permit ip dhcpsnooping any
```

Related Commands

access-list hardware (named)

show access-list (IPv4 Hardware ACLs)

show ip dhcp snooping agent-option

Overview Use this command to display DHCP snooping Option 82 information for all interfaces, a specific interface or a range of interfaces.

Syntax `show ip dhcp snooping agent-option [interface <interface-list>]`

Parameter	Description
`interface`	Specify the interface.
`<interface-list>`	The name of the interface or interfaces.

Mode User Exec and Privileged Exec

Examples To display DHCP snooping Option 82 information for all interfaces, use the command:

```
awplus# show ip dhcp snooping agent-option
```

To display DHCP snooping Option 82 information for vlan1, use the command:

```
awplus# show ip dhcp snooping agent-option interface vlan1
```

To display DHCP snooping Option 82 information for port1.0.1, use the command:

```
awplus# show ip dhcp snooping agent-option interface port1.0.1
```

Output Figure 35-1: Example output from the **show ip dhcp snooping agent-option** command

```
awplus#show ip dhcp snooping agent-option

DHCP Snooping Option 82 Configuration:

  Key:      C Id = Circuit Id Format
            R Id = Remote Id
            S Id = Subscriber Id

  Option 82 insertion ............... Enabled
  Option 82 on untrusted ports ...... Not allowed

-----------------------------------------------------------------
 vlan1       C Id = vlanifindex
             R Id = Access-Island-01-M1
 vlan2       C Id = vlantriplet
             R Id = Access-Island-01-M1
 vlan3       C Id = vlantriplet
             R Id = Access-Island-01-M3
 vlan4       C Id = vlantriplet
             R Id = 0000.cd28.074c
 vlan5       C Id = vlantriplet
             R Id = 0000.cd28.074c
 vlan6       C Id = vlantriplet
             R Id = 0000.cd28.074c
 port1.0.1   S Id =
 port1.0.2   S Id =
 port1.0.3   S Id = phone_1
 port1.0.4   S Id =
 port1.0.5   S Id = PC_1
 port1.0.6   S Id = phone_2
```

Related Commands

ip dhcp snooping agent-option

ip dhcp snooping agent-option circuit-id vlantriplet

ip dhcp snooping agent-option remote-id

show ip dhcp snooping

show ip dhcp snooping interface

show ip dhcp snooping binding

Overview Use this command to display all dynamic and static entries in the DHCP snooping binding database.

Syntax

```
show ip dhcp snooping binding
```

Mode User Exec and Privileged Exec

Example To display entries in the DHCP snooping database, use the command:

```
awplus# show ip dhcp snooping binding
```

Table 14: Example output from the **show ip dhcp snooping binding** command

```
awplus# show ip dhcp snooping binding
DHCP Snooping Bindings:

Client           MAC              Server                        Expires
IP Address       Address          IP Address       VLAN  Port   (sec)       Type
-------------------------------------------------------------------------------
1.2.3.4          aaaa.bbbb.cccc   --               7     1.0.6   Infinite   Stat
1.2.3.6          any              --               4077  1.0.6   Infinite   Stat
1.3.4.5          any              --               1     sa1     Infinite   Stat
111.111.100.101  0000.0000.0001   111.112.1.1      1     1.0.6   4076       Dyna
111.111.101.108  0000.0000.0108   111.112.1.1      1     1.0.6   4084       Dyna
111.111.101.109  0000.0000.0109   111.112.1.1      1     1.0.6   4085       Dyna
111.211.100.101  --               --               1     1.0.2   2147483325 Dyna
111.211.100.109  00b0.0000.0009   111.112.111.111  1     1.0.2   21         Dyna
111.211.101.101  00b0.0000.0101   111.112.111.111  1     1.0.2   214        Dyna

Total number of bindings in database: 9
```

Table 15: Parameters in the output from the **show ip dhcp snooping binding** command

Parameter	Description
Client IPAddress	The IP address of the DHCP client.
MAC Address	The MAC address of the DHCP client.
Server IP	The IP address of the DHCP server.
VLAN	The VLAN associated with this entry.
Port	The port the client is connected to.
Expires (sec)	The time in seconds until the lease expires.

Table 15: Parameters in the output from the **show ip dhcp snooping binding** command (cont.)

Parameter	Description
`Type`	The source of the entry: • Dyna: dynamically entered by snooping DHCP traffic, configured by the ip dhcp snooping binding command, or loaded from the database backup file. • Stat: added statically by the ip source binding command
`Total number of bindings in database`	The total number of dynamic and static lease entries in the DHCP snooping database.

Related Commands

ip dhcp snooping binding

ip dhcp snooping max-bindings

show ip source binding

show ip dhcp snooping interface

Overview Use this command to display information about DHCP snooping configuration and leases for the specified ports, or all ports.

Syntax `show ip dhcp snooping interface [<port-list>]`

Parameter	Description
<port-list>	The ports to display DHCP snooping configuration information for. If no ports are specified, information for all ports is displayed.

Mode User Exec and Privileged Exec

Example To display DHCP snooping information for all ports, use the command:

```
awplus# show ip dhcp snooping interface
```

Table 16: Example output from the **show ip dhcp snooping interface** command

```
awplus#show ip dhcp snooping interface

DHCP Snooping Port Status and Configuration:

  Port: Provisioned ports marked with brackets, e.g. (portx.y.z)
  Action: LG = Log
          TR = Trap
          LD = Link down

                        Full    Max
 Port         Status     Leases  Leases  Action     Subscriber-ID
-------------------------------------------------------------------------------
 port1.0.1    Untrusted  1       1       LG -- --
 port1.0.2    Untrusted  0       50      LG TR LD   Building 1 Level 1
 port1.0.3    Untrusted  0       50      LG -- --
 port1.0.4    Untrusted  0       50      LG -- --   Building 1 Level 2
 port1.0.5    Untrusted  0       50      LG -- LD   Building 2 Level 1
 port1.0.6    Untrusted  0       1       LG -- --
 port1.0.7    Untrusted  0       1       LG -- --
 port1.0.8    Untrusted  0       1       LG -- --
 port1.0.9    Untrusted  0       1       -- TR --
 port1.0.10   Untrusted  0       1       -- -- LD
 port1.0.11   Trusted    0       1       -- -- --
 port1.0.12   Trusted    0       1       -- -- --
```

Table 17: Parameters in the output from the **show ip dhcp snooping interface** command

Parameter	Description
`Port`	The port interface name.
`Status`	The port status: untrusted (default) or trusted.
`Full Leases`	The number of entries in the DHCP snooping database for the port.
`Max Leases`	The maximum number of entries that can be stored in the database for the port.
`Action`	The DHCP snooping violation actions for the port.
`Subscriber ID`	The subscriber ID for the port. If the subscriber ID is longer than 34 characters, only the first 34 characters are displayed. To display the whole subscriber ID, use the show running-config dhcp command.

Related Commands

show ip dhcp snooping

show ip dhcp snooping statistics

show running-config dhcp

show ip dhcp snooping statistics

Overview Use this command to display DHCP snooping statistics.

Syntax

```
show ip dhcp snooping statistics [detail] [interface
<interface-list>]
```

Parameter	Description
`detail`	Display detailed statistics.
`interface <interface-list>`	Display statistics for the specified interfaces. The interface list can contain switch ports, static or dynamic link aggregators (channel groups), or VLANs.

Mode User Exec and Privileged Exec

Example To show the current DHCP snooping statistics for all interfaces, use the command:

```
awplus# show ip dhcp snooping statistics
```

Table 18: Example output from the **show ip dhcp snooping statistics** command

```
awplus# show ip dhcp snooping statistics

DHCP Snooping Statistics:
              In BOOTP     In BOOTP     In          In
 Interface    Packets      Requests      Replies    Discards
-------------------------------------------------------------
 vlan1        444          386           58           223
 port1.0.1    386          386           0            223
 port1.0.2    0            0             0            0
 port1.0.3    0            0             0            0
 port1.0.4    0            0             0            0
 port1.0.5    0            0             0            0
 port1.0.6    58           0             58           0
```

Table 19: Example output from the **show ip dhcp snooping statistics detail** command

```
awplus# show ip dhcp snooping statistics detail

DHCP Snooping Statistics:
Interface ....................................... port1.0.1, All counters 0
Interface ....................................... port1.0.2, All counters 0
Interface ....................................... port1.0.3, All counters 0
Interface ....................................... port1.0.4
  In Packets ..................................... 50
    In BOOTP Requests ............................ 25
    In BOOTP Replies ............................. 25
  In Discards .................................... 1
    Invalid BOOTP Information .................... 0
    Invalid DHCP ACK ............................. 0
    Invalid DHCP Release or Decline .............. 0
    Invalid IP/UDP Header ........................ 0
    Max Bindings Exceeded ........................ 1

  Option 82 Insert Error ....................... 0

  Option 82 Received Invalid ................... 0

  Option 82 Received On Untrusted Port ......... 0

  Option 82 Transmit On Untrusted Port ......... 0
    Reply Received On Untrusted Port ............. 0
    Source MAC/CHADDR Mismatch ................... 0
    Static Entry Already Exists .................. 0
Interface ....................................... port1.0.5, All counters 0
Interface ....................................... port1.0.6, All counters 0
```

Table 20: Parameters in the output from the **show ip dhcp snooping statistics** command

Parameter	Description
`Interface`	The interface name.
`In Packets`	The total number of incoming packets that are processed by DHCP Snooping.
`In BOOTP Requests`	The total number of incoming BOOTP Requests.
`In BOOTP Replies`	The total number of incoming BOOTP Replies.
`In Discards`	The total number of incoming packets that have been discarded.
`Invalid BOOTP Information`	Packet contained invalid BOOTP information, such as an invalid BOOTP.OPCode.
`Invalid DHCP ACK`	A DHCP ACK message was discarded, for reasons such as missing Server Option or Lease Option.

Table 20: Parameters in the output from the **show ip dhcp snooping statistics** command (cont.)

Parameter	Description
`Invalid DHCP Release or Decline`	A DHCP Release or Decline message was discarded, for reasons such as mismatch between received interface and current binding information.
`Invalid IP/UDP Header`	A problem was detected in the IP or UDP header of the packet.
`Max Bindings Exceeded`	Accepting the packet would cause the maximum number of bindings on a port to be exceeded.
`Option 82 Insert Error`	An error occurred while trying to insert DHCP Relay Agent Option 82 information.
`Option 82 Received Invalid`	The DHCP Relay Agent Option 82 information received did not match the information inserted by DHCP Snooping.
`Option 82 Received On Untrusted Port`	A packet containing DHCP Relay Agent Option 82 information was received on an untrusted port.
`Option 82 Transmit On Untrusted Port`	A packet containing DHCP Relay Agent Option 82 information was to be sent on an untrusted port.
`Reply Received On Untrusted Port`	A BOOTP reply was received on an untrusted port.
`Source MAC/CHADDR Mismatch`	The L2 Source MAC address of the packet did not match the client hardware address field (BOOTP.CHADDR).
`Static Entry Already Exists`	An entry could not be added as a static entry already exists.

Related Commands

clear ip dhcp snooping statistics

ip dhcp snooping

ip dhcp snooping violation

show ip source binding

Overview Use this command to display static entries in the DHCP snooping database. These are the entries that have been added by using the ip source binding command.

Syntax

```
show ip source binding
```

Mode User Exec and Privileged Exec

Example To display static entries in the DHCP snooping database information, use the command:

```
awplus# show ip source binding
```

Table 21: Example output from the **show ip source binding** command

```
awplus# show ip source binding

IP Source Bindings:

Client       MAC                                Expires
IP Address   Address         VLAN  Port         (sec)      Type
-------------------------------------------------------------------
 1.1.1.1     0000.1111.2222  1     port1.0.1    Infinite   Static
```

Table 22: Parameters in the output from the **show ip source binding** command

Parameter	Description
Client IP Address	The IP address of the DHCP client.
MAC Address	The MAC address of the DHCP client.
VLAN	The VLAN ID the packet is received on.
Port	The Layer 2 port name the packet is received on.
Expires (sec)	Always infinite for static bindings, or when the leave time in the DHCP message was 0xffffffff (infinite).
Type	DHCP Snooping binding type: Static

Related Commands

ip source binding

show ip dhcp snooping binding

36 OpenFlow Commands

Introduction

Overview This chapter provides an alphabetical reference of commands used to configure *OpenFlow*.

The table below lists the OpenFlow commands and their applicable modes.

Figure 36-1: OpenFlow commands and applicable modes

Mode	Command
User Exec/Privileged Exec	show openflow config
	show openflow coverage
	show openflow flows
	show openflow rules
	show openflow status
Global Configuration	openflow controller
	openflow native vlan
	openflow version
Port Interface	openflow

Command List

openflow

Overview Use this command to specify a port as a data plane port. The ingress and egress traffic on the data plane port become controlled by the OpenFlow Controller. A data plane port number is assigned to the port automatically.

Use the **no** variant of this command to cancel the setting of a port as a data plane port. After entering the **no** variant of this command, you must restart the switch.

Syntax

```
openflow
no openflow
```

Default All the ports are non-data plane ports by default.

Mode Port Interface mode

Example To specify port1.0.3 as a data plane port:

```
awplus# configure terminal
awplus(config)# interface port1.0.3
awplus(config-if)# openflow
```

Related Commands show openflow config

openflow controller

Overview Use this command to specify the IPv4 address of the OpenFlow controller and the TCP port number. An OpenFlow switch forwards packets on the data plane ports based on the flow entries sent by the OpenFlow controller specified by this command.

You can specify one or more OpenFlow controllers to the switch.

Use the **no** variant of this command to delete one or more OpenFlow controllers specified to the switch.

Syntax

```
openflow controller <protocol> <controller_ip_address>
<1-65535>
```

Parameter	Description
<protocol>	The protocol type to communicate with the OpenFlow controller. The option is only TCP.
<controller_ip_address>	The IPv4 address of the OpenFlow controller
<1-65535>	The port number of TCP

Default No OpenFlow controller is configured by default.

Mode Global Configuration

Example To set the OpenFlow controller with the IPv4 address 10.1.1.1 and the TCP port number 6653:

```
awplus# configure terminal
awplus(config)# openflow controller tcp 10.1.1.1 6653
```

Related Commands show openflow config

openflow native vlan

Overview Use this command to specify a VLAN as a native VLAN for the data plane ports. You must create a VLAN using the vlan database command before specifying the VLAN as a native VLAN.

Use the **no** variant of this command to change the native VLAN for the data plane ports back to the default VLAN 1.

Syntax

```
openflow native vlan <1-4090>
no openflow native vlan
```

Parameter	Description
<vlan_id>	VLAN ID in the range <1-4090>

Default The native VLAN for the data plane ports is VLAN 1 by default.

Mode Global Configuration

Example To specify VLAN 100 as a native VLAN for the data plane ports:

```
awplus# configure terminal
awplus(config)# openflow native vlan 100
```

To change the native VLAN for the data plane ports back to the VLAN 1:

```
awplus# configure terminal
awplus(config)# no openflow native vlan
```

Related Commands show openflow config

openflow version

Overview Use this command to change the supported OpenFlow version numbers on the switch. You can specify a list of version numbers.

Use the **no** variant of this command to change the version number of the OpenFlow protocol back to the default version 1.3.

Syntax

```
openflow version <version-list>
no openflow version <version-list>
```

Parameter	Description
<version-list>	Specifies a list of version numbers separated by a space. The version numbers are 1.0 and 1.3.

Default The OpenFlow version is set to 1.3 by default.

Mode Global Configuration

Example To change the OpenFlow protocol version to 1.0 and 1.3:

```
awplus(config)# openflow version 1.0 1.3
```

To change the OpenFlow protocol version to the default 1.3:

```
awplus(config)# no openflow version
```

Related Commands show openflow config

show openflow config

Overview Use this command to display the OpenFlow configuration database on the switch.

Syntax

```
show openflow config
```

Mode User Exec/Privileged Exec

Example To show the contents of the OpenFlow configuration database on the switch:

```
awplus# show openflow config
```

Output Figure 36-2: Example output from **show openflow config**

```
awplus# show openflow config
fdf075ee-7485-4588-9885-1f0333df89a2
    Bridge "br0"
        Controller "tcp:192.168.1.2:6653"
            is_connected: true
        fail_mode: secure
        Port "port1.0.4"
            Interface "port1.0.4"
                type: system
                options: {ifindex="5004", mtu="1500",
native_vlan="4090"}
        Port "port1.0.3"
            Interface "port1.0.3"
                type: system
                options: {ifindex="5003", mtu="1500",
native_vlan="4090"}
        Port "br0"
            Interface "br0"
                type: internal
        Port "port1.0.1"
            Interface "port1.0.1"
                type: system
                options: {ifindex="5001", mtu="1500",
native_vlan="4090"}
        Port "port1.0.2"
            Interface "port1.0.2"
                type: system
                options: {ifindex="5002", mtu="1500",
native_vlan="4090"}
```

Table 36-1: Parameters in the output from **show openflow config**

Parameter	Description
`First line`	The switch ID
`Bridge "br0"`	The configuration of Bridge "br0"

Table 36-1: Parameters in the output from **show openflow config** (cont.)

Parameter	Description
`Controller`	The IPv4 address of the OpenFlow controller and TCP port number
`fail_mode`	The fail mode. When the fail mode is "secure," OpenFlow on the switch does not set up flows when the OpenFlow controller fails.
`is_connected`	Whether or not the OpenFlow controller is connected
`Port`	The port information
`Interface`	The interface of the port.
`type:`	The type of the port
`options:`	The options for the port

Related Commands

openflow controller

openflow native vlan

show openflow status

show openflow coverage

Overview Use this command to display the OpenFlow counters from the Open vSwitch kernel module.

Syntax

```
show openflow coverage
```

Mode User Exec/Privileged Exec

Usage The information displayed by this command is for troubleshooting. Contact Allied Telesis Technical Support for assistance.

Example To show OpenFlow counters:

```
awplus# show openflow coverage
```

Output Figure 36-3: Example output from **show openflow coverage**

```
awplus# show openflow coverage
Event coverage, avg rate over last: 5 seconds, last minute, last hour,
hash=86bbd699:netlink_sent               0.0/sec     0.000/sec        0.0000/sec
total: 14
netlink_recv_jumbo         0.0/sec     0.000/sec        0.0000/sec   total: 4
netlink_received           0.0/sec     0.000/sec        0.0000/sec   total: 49
nln_changed                0.0/sec     0.000/sec        0.0000/sec   total: 18
vconn_sent                 0.0/sec     0.000/sec        0.4703/sec   total: 1801
vconn_received             0.0/sec     0.000/sec        0.4594/sec   total: 1768
vconn_open                 0.4/sec     0.267/sec        0.2372/sec   total: 876
util_xalloc              370.2/sec   354.183/sec      416.7711/sec   total: 1590959
unixctl_replied            0.0/sec     0.017/sec        0.0028/sec   total: 10
unixctl_received           0.0/sec     0.017/sec        0.0028/sec   total: 10
stream_open                0.4/sec     0.267/sec        0.2372/sec   total: 877
pstream_open               0.0/sec     0.000/sec        0.0000/sec   total: 6
rconn_sent                 0.0/sec     0.000/sec        0.4219/sec   total: 1606
rconn_queued               0.0/sec     0.000/sec        0.4219/sec   total: 1606
poll_zero_timeout          0.0/sec     0.033/sec        0.0875/sec   total: 362
poll_create_node          60.6/sec    55.967/sec       68.2844/sec   total: 256721
txn_success                0.2/sec     0.200/sec        0.1953/sec   total: 734
txn_incomplete             0.2/sec     0.267/sec        0.2622/sec   total: 994
txn_unchanged              0.0/sec     0.000/sec        0.0019/sec   total: 34
netdev_get_stats           1.2/sec     1.200/sec        1.1850/sec   total: 4411
netdev_sent                0.0/sec     0.000/sec        0.1219/sec   total: 475
netdev_received            0.0/sec     0.000/sec        0.2608/sec   total: 1005
hmap_expand               10.0/sec     9.433/sec       11.0714/sec   total: 42476
hmap_pathological          0.0/sec     0.000/sec        0.0000/sec   total: 58
hindex_expand              0.0/sec     0.000/sec        0.0006/sec   total: 3
miniflow_malloc            0.0/sec     0.000/sec        0.2611/sec   total: 1008
flow_extract               0.0/sec     0.000/sec        0.0006/sec   total: 5
```

```
dpif_flow_del              0.0/sec     0.000/sec        0.1342/sec   total: 516
dpif_flow_put              0.0/sec     0.000/sec        0.0014/sec   total: 5
dpif_flow_flush            0.0/sec     0.000/sec        0.0000/sec   total: 2
dpif_port_add              0.0/sec     0.000/sec        0.0000/sec   total: 25
cmap_shrink                0.0/sec     0.000/sec        0.2939/sec   total: 1157
cmap_expand                0.0/sec     0.000/sec        0.0006/sec   total: 3
ttp_rev_flow_table         0.0/sec     0.000/sec        0.1050/sec   total: 410
ttp_rev_port_toggled       0.0/sec     0.000/sec        0.0000/sec   total: 2
ttp_rev_reconfigure        0.0/sec     0.000/sec        0.0006/sec   total: 20
xlate_actions              0.0/sec     0.000/sec        0.3969/sec   total: 1530
revalidate_missed_dp_flow   0.0/sec     0.000/sec         0.1356/sec   total: 521
handler_duplicate_upcall   0.0/sec     0.000/sec        0.1258/sec   total: 483
ofproto_update_port        0.0/sec     0.000/sec        0.0000/sec   total: 29
ofproto_recv_openflow      0.0/sec     0.000/sec        0.4111/sec   total: 1573
ofproto_queue_req          0.0/sec     0.000/sec        0.0003/sec   total: 1
ofproto_packet_out         0.0/sec     0.000/sec        0.0006/sec   total: 4
ofproto_flush              0.0/sec     0.000/sec        0.0000/sec   total: 1
bridge_reconfigure         0.0/sec     0.000/sec        0.0000/sec   total: 19
72 events never hit
```

Table 36-2: Parameters in the output from

Parameter	Description
`Event coverage`	The name of a coverage event
`avg rate over last: 5 seconds`	The rate at which the event occurred for the alast 5 seconds
`last minute`	The rate at which the event occurred for the last one minute
`last hour`	The rate at which the event occurred for the last one hour
`hash`	The name of the internal hash on the counter
`total:`	The total occurrence of the event.
`events never hit`	The number of coverage events that have never occurred. When the value is 0, this information is not displayed.

Related Commands

show openflow status

show openflow flows

show openflow flows

Overview Use this command to display the entries of the flow table on the switch.

Syntax

```
show openflow flows
```

Mode User Exec/Privileged Exec

Example To show the entries of the flow table on the switch:

```
awplus# show openflow flows
```

Output Figure 36-4: Example output from **show openflow flows**

```
awplus# show openflow flows
recirc_id(0),in_port(4),eth(src=00:23:45:67:89:ab,dst=00:de:f0:12:
34:56),eth_type(0x0800),ipv4(frag=no), packets:2, bytes:692,
used:2.436s,
actions:1recirc_id(0),in_port(1),eth(src=00:23:45:67:89:ab/00:01:0
0:00:00:00,dst=00:de:f0:12:34:56),eth_type(0x0800),ipv4(frag=no),
packets:2, bytes:692, used:2.435s,
actions:4recirc_id(0),in_port(1),eth(src=00:23:45:67:89:ab/00:01:0
0:00:00:00,dst=00:de:f0:12:34:56),eth_type(0x0806), packets:0,
bytes:0, used:never,
actions:4recirc_id(0),in_port(4),eth(src=00:23:45:67:89:ab,dst=00:
de:f0:12:34:56),eth_type(0x0806), packets:0, bytes:0, used:never,
actions:1
```

Table 36-3: Parameters in the output from **show openflow flows**

Parameter	Description
recirc_id	The recirc ID
in_port	The port number of the OpenFlow port
eth	The source and destination MAC address of the packet
eth_type	The Ethernet type
ipv4	The information in the IPv4 header
packets	The number of matched packets
bytes	The number of matched bytes
actions	A set of actions for the packets that match the key

Related Commands

show openflow coverage

show openflow rules

show openflow rules

Overview Use this command to display the software flow table and rules set by the OpenFlow controller.

Syntax

```
show openflow rules
```

Mode User Exec/Privileged Exec

Example To show the contents of the flow table on the switch:

```
awplus# show openflow rules
```

Output Figure 36-5: Example output from **show openflow rules**

```
awplus# show openflow rules
duration=14s, n_packets=0, n_bytes=0,
priority=399,in_port=1,dl_src=ec:cd:6d:c4:21:bd,actions=dropdurati
on=14s, n_packets=0, n_bytes=0,
priority=399,in_port=2,dl_src=ec:cd:6d:c4:21:bd,actions=dropdurati
on=14s, n_packets=0, n_bytes=0,
priority=399,in_port=3,dl_src=ec:cd:6d:c4:21:bd,actions=dropdurati
on=14s, n_packets=0, n_bytes=0,
priority=399,in_port=4,dl_src=ec:cd:6d:c4:21:bd,actions=dropdurati
on=14s, n_packets=0, n_bytes=0,
priority=299,in_port=1,dl_dst=00:00:00:00:00:00/01:00:00:00:00:00,
actions=goto_table:2duration=14s, n_packets=0, n_bytes=0,
priority=298,in_port=1,actions=goto_table:3duration=14s,
n_packets=0, n_bytes=0,
priority=99,arp,actions=CONTROLLER:65535duration=14s, n_packets=0,
n_bytes=0,
priority=99,udp,tp_dst=67,actions=CONTROLLER:65535duration=14s,
n_packets=0, n_bytes=0, priority=0,actions=droptable_id=1,
duration=14s, n_packets=0, n_bytes=0,
priority=99,dl_dst=00:00:00:00:00:00/01:00:00:00:00:00,actions=got
o_table:2table_id=1, duration=14s, n_packets=0, n_bytes=0,
priority=0,actions=droptable_id=2, duration=14s, n_packets=0,
n_bytes=0, priority=98,in_port=1,actions=droptable_id=2,
duration=14s, n_packets=0, n_bytes=0,
priority=97,actions=output:1table_id=2, duration=14s, n_packets=0,
n_bytes=0, priority=0,actions=droptable_id=3, duration=14s,
n_packets=0, n_bytes=0, priority=0,actions=droptable_id=254,
duration=85668s, n_packets=0, n_bytes=0,
priority=2,recirc_id=0,actions=droptable_id=254, duration=85668s,
n_packets=736, n_bytes=144050,
priority=0,reg0=0x1,actions=controller(reason=no_match)table_id=25
4, duration=85668s, n_packets=19, n_bytes=5668,
priority=0,reg0=0x2,actions=drop
```

Table 36-4: Parameters in the output from **show openflow rules**

Parameter	Description
duration	The duration of the flow entry in seconds
n_packets	The number of packets that match the flow entry
n_bytes	The number of bytes that match the flow entry
priority	The priority of the flow entry
in_port	The OpenFlow port number on which the packets are received
dl_src	The source address
dl_dst	The destination address
actions	A set of actions applied to a packet. The actions are: “drop”, “goto_table”, “pop_vlan”, or “push_vlan”
table_id	The table ID of the flow entry

Related Commands

show openflow flows

show openflow coverage

show openflow status

Overview Use this command to display the status of each data plane port and the OpenFlow protocol messages queried d by the OpenFlow controller.

Syntax

```
show openflow status
```

Mode User Exec/Privileged Exec

Example To show the status for each data plane port and OpenFlow protocol messages:

```
awplus# show openflow status
```

Output Figure 36-6: Example output from **show openflow status**

```
awplus#show openflow status
 OFPT_FEATURES_REPLY (OF1.3) (xid=0x2): dpid:0000eccd6dc421bd
n_tables:254, n_buffers:256
capabilities: FLOW_STATS TABLE_STATS PORT_STATS GROUP_STATS
QUEUE_STATS
OFPST_PORT_DESC reply (OF1.3) (xid=0x3):
 1(port1.0.1): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      0
     current:    1GB-FD
     supported:  1GB-FD
     speed: 1000 Mbps now, 1000 Mbps max
 2(port1.0.2): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      LINK_DOWN
     current:    AUTO_NEG
     supported:  1GB-FD
     speed: 0 Mbps now, 1000 Mbps max
 3(port1.0.3): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      0
     current:    1GB-FD
     supported:  1GB-FD
     speed: 1000 Mbps now, 1000 Mbps max
 4(port1.0.4): addr:ec:cd:6d:c4:21:bd
     config:     0
     state:      LINK_DOWN
     current:    AUTO_NEG
     supported:  1GB-FD
     speed: 0 Mbps now, 1000 Mbps max
OFPT_GET_CONFIG_REPLY (OF1.3) (xid=0x5): frags=normal
miss_send_len=0
```

Table 36-5: Parameters in the output from **show openflow status**

Parameter	Description
`Parameter 2`	Description of parameter 2.
`OFPT_FEATURES_REPLY (OF1.3) (xid=0x2):`	Indicates that the following information is from the OpenFlow version 1.3 Feature reply.
`dpid:`	The datapath ID
`n_tables`	The number of tables supported by the switch
`n_buffers`	The maximum number of packets that the switch can buffer when sending packets to the OpenFlow controller
`capabilities`	A list of the OpenFlow capabilities:: FLOW_STATS (flow statistics), TABLE_STATS (table statistics), PORT_STATS (port statistics), IP_REASM (IP fragments reassemble), QUEUE_STATS (queue statistics), and GROUP_STATS (group statistics
`OFPST_PORT_DESC replay (OF1.3) (xid=0x3):`	Indicates that the following information is from the OpenFlow version 1.3 Port Description Reply.
`1(port1.0.1): addr:ec:cd:6d:c4:21:bd`	The port number and Mac address.
`config:`	The port status: 0 (the port is up) or PORT_DOWN (the port is down.)
`state:`	The link status: 0 (the link is up) or LINK_DOWN (the link is down.)
`current:`	The current feature status.
`supported:`	A list of the supported features:: 1GB-FD, 10GB-FD, AUTO-NEG, etc.
`speed:`	The current port speed and maximum speed.
`OFPT_GET_CONFIG_REPLY (OF1.3) (xid=0x5):`	Indicates that the switch responds to a configuration request by an OFPT_GET_CONFIG_REPLY message with the following information.
`frags:`	The action for the IP fragments: normal, dropped, or reassembled. Normal means that an attempt should be made to pass the fragments through the OpenFlow tables.
`miss_send_len=0:`	The number of bytes of each packet that was sent to the OpenFlow controller when a flow table fails or reaches the controller

Related Commands

show openflow flows

show openflow rules

Part 6: Network Availability

37 Virtual Chassis Stacking (VCStack™) Commands

Introduction

Overview This chapter provides an alphabetical reference for Virtual Chassis Stacking (VCStack™) commands.

For information on stacking, see VCStack Feature Overview and Configuration Guide.

Also note the following stacking trigger commands that are documented in the Triggers chapter:

type stack disabled-master command

type stack master-fail command

type stack member command

type stack link command

In addition to the stacking commands shown in this chapter, stacking content also exists in the following commands:

hostname command

reboot command

reload command

show cpu command

show cpu history command

show exception log command

show file systems command

show memory command

show memory history command

show process command

show system command

CAUTION: *Stack operation is only supported if* ***stack virtual-mac*** *is enabled. For more information refer to stack virtual-mac on page 1459*

Command List

clear counter stack

Overview This command clears all stack counters for all stack members.

Syntax

```
clear counter stack
```

Mode Privileged Exec

Example To clear all stack counters:

```
awplus# clear counter stack
```

Related Commands show counter stack

debug stack

Overview This command enables the stacking debugging facilities.

Syntax

```
debug stack [link|topology|trace]
no debug stack [link|topology|trace]
```

Parameter	Description
`link`	Stacking neighbor discovery events on stack links.
`topology`	Stacking topology discovery messages.
`trace`	Notable stacking events.

Default Stack trace debugging is enabled.

Mode Privileged Exec and Global Configuration

Usage The command displays debug information about the stacked devices. If no parameter is specified, all the stack debugging information will be displayed, including link events, topology discovery messages and all notable stacking events. If link parameter is specified, only the link events debugging information will be displayed.

Examples To enable debugging, enter the following command on the stack master:

```
awplus# debug stack
```

To enable link debugging, enter the following command on the stack master:

```
awplus# debug stack link
```

To enable topology discovery debugging, enter the following command on the stack master:

```
awplus# debug stack topology
```

To enable stack trace debugging, enter the following command on the stack master:

```
awplus# debug stack trace
```

Related Commands undebug stack

reboot rolling

Overview This command reboots a stack in a rolling sequence to minimize downtime.

The stack master is rebooted, causing the remaining stack members to failover and elect a new master. The rebooted unit remains separate from the remaining stack and boots up as a stand-alone unit. Once the rebooted unit has finished running its configuration and has brought its ports up, it reboots all the remaining stack members at once.

Syntax

```
reboot rolling
```

Mode Privileged Exec

Usage If you are upgrading to a new software version, the new version must also support rollling reboot.

NOTE: *When stacking is used with EPSR, the EPSR **failovertime** must be set to at least 5 seconds to avoid any broadcast storms during failover. Broadcast storms may occur if the switch cannot failover quickly enough before the EPSR **failovertime** expires. For further information about EPSR **failovertime**, see the epsr command.*

Examples To rolling reboot the stack, use the following commands:

```
awplus# reboot rolling
Continue the rolling reboot of the stack? (y/n):
```

After running this command, the stack master will reboot immediately with the configuration file settings. The remaining stack members will then reboot once the master has finished re-configuring.

```
Continue the rolling reboot of the stack? (y/n):
awplus# y
```

Related Commands boot system

epsr

reload rolling

Overview This command performs the same function as the reboot rolling command.

remote-command (deleted)

Overview This command has been deleted in Software Version 5.4.4-1.1 and later. Instead, please use the remote-login command and then run the command you need to run remotely.

remote-login

Overview This command is used only on the master in order to log onto the CLI of another stack member. In most respects the result of this is similar to being logged into the stack master. Configuration commands are still applied to all stack members, but show commands, and commands that access the file system are executed locally.

The specific output obtained will vary greatly depending on the show command chosen.

Syntax `remote-login <stack-ID>`

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.

Mode Privileged Exec

Usage Note that some commands such as **ping** or **telnet** are not available when the remote- login is used.

Example To log onto stack member 2, use the following command:

```
awplus# remote-login 2
```

To return to the command prompt on the master stack member, type **exit**.

show counter stack

Overview Use this command to display stack related counter information.

Syntax

```
show counter stack
```

Default All counters are reset when the stack member is rebooted.

Mode User Exec and Privileged Exec

Usage This displays the stacking counter information for every stack member.

Examples To display the stacking counter information about the whole stack, use the following command.

```
awplus# show counter stack
```

Table 37-1: Example output from the **show counter stack** command

```
Virtual Chassis Stacking counters

Stack member 1:

Topology Event counters
Units joined          .........1
Units left            .........0
Links up              .........1
Links down            .........0
ID conflict           .........0
Master conflict       .........0
Master failover       .........0
Master elected        .........1
Master discovered     .........0
SW autoupgrades       .........0

Stack Port 1 Topology Event counters
Link up               .........3
Link down             .........2
Nbr re-init           .........0
Nbr incompatible      .........0
Nbr 2way comms        .........1
Nbr full comms        .........1

Stack Port 2 Topology Event counters
Link up               .........0
Link down             .........0
Nbr re-init           .........0
Nbr incompatible      .........0
Nbr 2way comms        .........0
Nbr full comms        .........0
```

Table 37-1: Example output from the **show counter stack** command (cont.)

```
Topology Message counters
Tx Total              .........4
Tx Hellos             .........4
Tx Topo DB            .........0
Tx Topo update        .........0
Tx Link event         .........0
Tx Reinitialise       .........0
Tx Port 1             .........4
Tx Port 2             .........0
Tx 1-hop transport    .........4
Tx Layer-2 transport  .........0
Rx Total              .........1
Rx Hellos             .........1
Rx Topo DB            .........0
Rx Topo update        .........0
Rx Link event         .........0
Rx Reinitialise       .........0
Rx Port 1             .........1
Rx Port 2             .........0
Rx 1-hop transport    .........1
Rx Layer-2 transport  .........0

Topology Error counters
Version unsupported   .........0
Product unsupported   .........0
XEM unsupported       .........0
Too many units        .........0
Invalid messages      .........0

Resiliency Link counters
Health status good    .........1
Health status bad     .........0
Tx                    .........0
Tx Error              .........0
Rx                    ......3600
Rx Error              .........0

Stack member 2:

-- Output repeated for other stack members - details not shown --
```

Table 38: Parameters in the output of the **show counter stack** command

Parameters	Description
Topology Event Counters	
`Units joined`	Number of times that the stack acquires a member.
`Units left`	Number of times that the stack loses a member.
`Links up`	Number of times that a stack link is up in the stack.
`Links down`	Number of times that a stack link is down in the stack.

Table 38: Parameters in the output of the **show counter stack** command (cont.)

Parameters	Description
ID conflict	Number of times that stack-ID conflicts.
Master conflict	Number of times that stack master conflict occurs.
Master failover	Number of times that stack master fails.
Master elected	Number of times that stack master is elected.
Master discovered	Number of times that stack master is discovered.
SW autoupgrades	Number of times that the software in the stack members are auto upgraded.
Stack port	
Link up	Number of times that this unit's physical stack link has come up.
Link down	Number of times that this unit's physical stack link has come down.
Nbr re-init	Number of times that the neighbor is detected as having reinitialised.
Nbr incompatible	Number of times that the neighbor is detected as incompatible.
Nbr 2way comms	Number of times that the neighbor is in two way communication status.
Nbr full comms	Number of times that the neighbor is in full communication status.
Topology message counters	
Total	Total number of topology messages.
Hellos	Number of hello messages.
Topology DB	Number of topology database messages.
Topology update	Number of topology database update messages.
Link event	Number of link event messages.
Reinitialise	Number of reinitialise messages.
1-hop transport	Number of 1-hop transport messages.
Layer-2 transport	Number of layer 2 transport messages.

Table 38: Parameters in the output of the **show counter stack** command (cont.)

Parameters	Description
`Link event`	Number of link event messages.
`Reinitialise`	Number of reinitialise messages.
`1-hop transport`	Number of 1-hop transport messages.
`Layer-2 transport`	Number of Layer 2 transport messages.
`Topology error counters`	Reasons why a neighboring unit could not join the stack.
`Version unsupported`	Number of stack software version unsupported errors.
`Product unsupported`	Number of product unsupported errors.
`XEM unsupported`	Number of XEM unsupported errors.
`Too many units`	Number of too many units errors.
`Invalid messages`	Number of invalid messages.
`Health status good`	The number of times that the resiliency link has successfully carried healthchecks following a failure at startup.
`Health status bad`	The number of times that the resiliency link healthcheck has timed out. A timeout occurs when a backup stack member detects a delay greater than two seconds between healthcheck messages received.
`Rx`	The total number of healthcheck messages that a stack member has received from the stack master.
`Rx Error`	The total number of invalid healthcheck messages that have been received from the master. This message is not applicable to the stack master.

Related Commands

show stack

switch provision (stack)

show debugging stack

Overview This command shows which debugging modes are currently enabled for stacking.

Syntax

```
show debugging stack
```

Mode User Exec and Privileged Exec

Example To display the stack debugging mode status, use the command:

```
awplus# show debugging stack
```

Figure 37-1: Example output from the **show debugging stack** command

```
Virtual Chassis Stacking debugging status:
  VCS link debugging is on
  VCS topology debugging is on
  VCS trace debugging is on
```

Related Commands debug stack

show running-config stack

Overview Use this command to display the running system information specific to the stack.

```
show running-config stack
```

Mode Privileged Exec and Global Configuration

Example To display the stacking running configuration information, use the command:

```
awplus# show running-config stack
```

Output Figure 37-2: Example output from the **show running-config stack** command

```
awplus#show running-config stack

stack virtual-mac
stack virtual-chassis-id 1982
stack management vlan 4000
stack management subnet 192.168.254.0
stack enable
stack 2 priority 20
```

Related Commands show running-config

show provisioning (stack)

Overview Use this command to display the provisioning status of all installed or provisioned hardware. Provisioning is the preconfiguration necessary to accommodate future connection of hardware items such as a switch.

Syntax

```
show provisioning
```

Mode User Exec and Privileged Exec

Example To show provisioning, use the following command:

```
awplus# show provisioning
```

Output Figure 37-3: Example output from the **show provisioning** command

```
Switch provisioning summary
information

ID  Board class Status
1.0 IX5-28      Hardware present
```

Table 39: Parameters in the output of the **show provisioning** command

Parameter	Description
ID	The unit bay-location of the hardware provision.
Board class	The hardware type.
Status	The provisioned state: • Hardware Present means that the hardware is currently installed in the stack. • Provisioned means that although the hardware is not currently installed, the stack is preconfigured ready to accept the hardware installation.

show stack

Overview Use this command to display summary information about current stack members.

Syntax

```
show stack
```

Mode User Exec and Privileged Exec

Usage This command displays summary information about current stack members. See show stack detail to display detailed stack information.

Example To display summary information about the stack, use the command:

```
awplus# show stack
```

Output Figure 37-4: Example output from the **show stack** command

```
Virtual Chassis Stacking summary information

ID  Pending ID  MAC address      Priority  Status  Role
1   -           0000.cd28.07e1   128       Ready   Active Master
2   -           0015.77c2.4d44   128       Ready   Backup Member
3   -           0015.77c9.7464   128       Syncing Backup Member
4   -           -                -         -       Provisioned

Operational Status                Normal operation
Stack MAC address                 0000.cd28.07e1
```

Table 40: Parameters in the output from the **show stack** command

Parameter	Description
ID	Stack-ID.
MAC address	Stack member MAC address.

Table 40: Parameters in the output from the **show stack** command (cont.)

Parameter	Description
`Priority`	Stack member master election priority (between 0 and 255). Note that the lowest number has the highest priority.
`Role`	Stack member's role in the stack, this can be one of: • **Active Master** • **Disabled Master**— this is the temporary master when there is a communication break within the stack, but communication still exists across the resiliency link. In this state all switch ports within the stack are disabled by default, but a different configuration can be run by a "type stack disabled-master" trigger. • **Backup Member**— a device other than the stack master. • **Provisioned**— indicates that the stack position is provisionally configured, i.e. ready to accept a particular switch type into the stack.

Related Commands

show stack detail

show counter stack

show stack resiliencylink

stack disabled-master-monitoring

stack resiliencylink

stack software-auto-synchronize

show stack detail

Overview Use this command to display detailed information about current stack members.

Syntax

```
show stack detail
```

Mode User Exec and Privileged Exec

Usage This command displays detailed information about current stack members. See show stack to display summary stack information only.

Example To display the detailed stacking information about the stack's overall status:

```
awplus# show stack detail
```

Figure 37-5: Example output from the **show stack detail** command

```
Virtual Chassis Stacking detailed information

Stack Status:
---------------------------------------------------------------
Operational Status Normal operation
Management VLAN ID 4094
Management VLAN subnet address 192.168.255.0
Virtual Chassis ID 388 (0x184)
Virtual MAC address 0000.cd37.0184
Mixed mode Disabled
Disabled Master Monitoring Enabled

Stack member 1:
---------------------------------------------------------------
ID 1
Pending ID -
MAC address 0000.cd28.070d
Last role change Wed May 7 22:31:58 2013
Product type IX5-28GPX
Role Active Master
Priority 1
Host name awplus
S/W version auto synchronizaion On
Resiliency link status Configured
Stack port 1.0.27 status learned neighbor 2
Stack port 1.0.28 status learned neighbor 3
```

```
Stack member 2:
-----------------------------------------------------------------
ID 2
Pending ID -
MAC address 0000.cd29.716d
Last role change Wed May 7 23:47:21 2013
Product type IX5-28GPX
Role Backup Member
Status Ready
Priority 2
Host name awplus-2
S/W version auto synchronization On
Resiliency link status Successful
Stack port 2.0.27 status learned neighbor 3
Stack port 2.0.28 status learned neighbor 1

Stack member 3:
-----------------------------------------------------------------
ID                                  3
Pending ID                          -
MAC address                         0015.77c2.4d9d
Last role change                    Wed May  7 22:31:58 2013
Product type                        IX5-28GPX
Role                                Backup Member
Priority                            3
Host name                           awplus-3
S/W version auto synchronizaion     On
Resiliency link status              Successful
Stack port 3.0.27 status            learned neighbor 1
Stack port 3.0.28 status            learned neighbor 2
```

Table 41: Parameters in the output from the **show stack detail** command

Parameter	Description
`S/W version auto synchronization`	Whether the software-auto-synchronization feature is turned on or off.
`Host name`	The host name of the stack member.
`ID`	Stack-ID.
`Last Role Change`	The date and time the stack member last changed its role in the stack.
`MAC address`	Stack member MAC address.
`Management VLAN ID`	The VLAN ID currently used for stack management: the default is 4094.
`Management VLAN subnet address`	The current stacking management VLAN subnet address.

Table 41: Parameters in the output from the **show stack detail** command (cont.)

Parameter	Description
`Virtual Chassis ID`	The Virtual Chassis ID determines the last 12 bits of the Virtual MAC address: `0000.cd37.0xxx`
`Virtual MAC Address`	The Virtual MAC address of the stack.
`Disabled Master Monitoring`	The current Disabled Master Monitoring status. This can be: • **Enabled** • **Disabled** • **Inactive**
`Operational Status`	The status of the stack. This can be: • **Normal operation**: If any other status is displayed, it may warrant further investigation. • **Stacking hardware disabled:** Use the **stack enable** command to activate the stacking feature. • **Operating in failover mode**: This stack member has become separated from the rest of the stack, or it failed to join the stack correctly. • **Standalone unit**: Stacking is enabled, but no other stack members are present. • **Not all stack ports are up**: One or more stacking ports may be down, or stacking discovery may not have detected the neighbor successfully.
`Stack Status`	The stack's overall status. Note that a warning is issued if the stack is not connected in a standard ring topology.
`Pending ID`	The pending stack member ID. This can be changed by the stack renumber command. If there is no pending ID, the "–" symbol will display.
`Stack port status`	The status of the stack port. This can be: • **Down** • **Neighbor incompatible** • **Discovering neighbor** • **Learned neighbor**
`Priority`	Stack member master election priority (between 1 and 255) Note that the lowest number has the highest priority.
`Product Type`	Stack member product type. For example, IX5- 28GPX.
`Provisioned`	Indicates that the stack position is provisionally configured, i.e. ready to accept a particular switch type into the stack.

Table 41: Parameters in the output from the **show stack detail** command (cont.)

Parameter	Description
`Resiliency` link status	The current status of the resiliency link. The status can be one of: • **Not configured** (Master or Member). • **Configured** (Master only). • **Successful**: Successfully receiving healthchecks from the Active Master. • **Failed** (Member only): Not receiving any healthchecks from the Active Master. • **Stopped**: The resiliency link is configured, but is inactive. This may occur in a Disabled Master stack, for example if the Disabled Master Monitoring feature is not used.
`Role`	Stack member's role in the stack, this can be one of: • **Active Master**. • **Disabled Master**— The temporary master when there is a communication break within the stack, but communication still exists across the resiliency link. In this state all switch ports within the stack are disabled by default, but a different configuration can be run by a "type stack disabled-master" trigger command. • **Backup Member**— a device other than the stack master. • **Discovering**— joining the stack.
`Status`	Indicates how readily a stack member can take over as master if the current stack master were to fail. • **Init —** the stack member is completing the startup initialization. • **Syncing**— the stack member is synchronizing state information with the stack master following startup. • **Ready**— the stack member is fully synchronized with the current master and is ready to take over immediately.

Related Commands

show stack

show counter stack

show stack resiliencylink

stack disabled-master-monitoring

stack resiliencylink

stack software-auto-synchronize

show stack resiliencylink

Overview Use this command to display information about the current status of the resiliency-link across the members of the stack.

Syntax show stack resiliencylink

Mode User Exec and Privileged Exec

Example To display information about the current status of the resiliency-link across the stack members, use the command:

```
awplus# show stack resiliencylink
```

Output Figure 37-6: Example output from the **show stack resiliencylink** command

```
awplus(config)# show stack resiliencylink
Stack member 1:
-------------------------------------------------------------
Status                          Configured
Interface                       vlan4093
Interface state                 UP
Resiliency-link port(s)         port1.2.11

Stack member 2:
-------------------------------------------------------------
Status                          Successful
Interface                       vlan4093
Interface state                 UP
Resiliency-link port(s)         port2.2.11
```

Table 42: Parameters in the output of the **show stack resiliencylink** command

Parameter	Description
`Status`	The current status of the stack member's resiliency link. Can be one of: • **Not configured** (Master or Member). • **Configured** (Master only). • **Successful**: Successfully receiving healthchecks from the Active Master. • **Failed** (Member only): Not receiving any healthchecks from the Active Master. • **Stopped**: The resiliency link is configured, but is inactive. This may occur in a Disabled Master stack, for example if the Disabled Master Monitoring feature is not used.
`Interface`	The name of the VLAN interface that is connected to the resiliency link.
`Interface state`	The current status of the interface. Can be either up or down.
`Resiliency-link port(s)`	The switch port(s) the resiliency link is connected to.

Related Commands

switch provision (stack)

show stack

stack resiliencylink

switchport resiliencylink

stack disabled-master-monitoring

Overview This command enables the Disabled Master Monitoring (DMM) feature. If a stack member becomes a disabled master, the DMM feature will use the stack resiliency link to continue monitoring the health of the separated stack master.

Use the **no** variant of this command to disable the DMM feature.

Syntax

```
stack disabled-master-monitoring
no stack disabled-master-monitoring
```

Default By default, Disabled Master Monitoring is enabled. However, it only operates if there is a resiliency link.

Mode Global Configuration

Usage This command enables additional stack resiliency link functionality, which is used if a stack separation occurs. For DMM to operate, a resiliency link must also be configured (stack resiliencylink command). A stack separation could result in a stack member becoming a disabled master, which has the configuration as a normal stack master except that all its switchports are shutdown.

For more information about the disabled master state, see the VCStack Feature Overview and Configuration Guide.

When the DMM feature is enabled, the disabled master will continue to monitor the health of the original stack master over the stack resiliency link connection. If the original stack master were to fail, when the DMM feature is enabled, then the disabled master will detect this and will automatically re-enable its switchports. This ensures that the stack will continue to pass network traffic, even if a catastrophic stack failure occurs.

For more information about the DMM feature when the stack member is a disabled master, see theVCStack Feature Overview and Configuration Guide.

Examples To enable the DMM feature, use the following commands:

```
awplus# configure terminal
awplus(config)# stack disabled-master-monitoring
```

To disable the DMM feature, use the following commands:

```
awplus# configure terminal
awplus(config)# no stack disabled-master-monitoring
```

Related Commands

switch provision (stack)

show stack

stack resiliencylink

type stack disabled-master

type stack master-fail

stack enable

Overview This command is used on a stackable stand-alone switch to manually turn on the VCStack feature.

This command can also be run on a switch that has previously been removed from a stack (by using the **no** variant of this command) and return it to stacking operation.

The **no** variant of this command removes a selected stack member switch, as specified by the <*stack-ID*> selection in the command syntax, from the virtual chassis stack.

Syntax

```
stack enable
no stack <stack-ID> enable
```

Parameter	Description
<*stack-ID*>	Stack member number, from 1 to 8.

Default The VCStack feature is enabled by default. The feature automatically starts when hardware is present.

Mode Global Configuration

Usage When stack enable is entered, the stack virtual-mac is automatically enabled. Using virtual-mac is required in order to minimize disruption on failover.

Running the **no** variant of this command will remove the selected stack member from the stack. At this point the removed member will act as a stand-alone master and will disable all of its ports. The switch can then only be accessed via its console port. If the command is run on the master then all current members of the stack will be disabled.

To return the switch to stack membership, first connect to the switch via its console port, then run the **stack enable** command. Then save the configuration and run the reboot command. This will reboot the switch and it will re-join the stack as an ordinary member.

If the switch was previously the stack master, you might want to return it to its original stack master status. To do this you must run the reboot command again. This time—because the switch is now a stack member—the command will reboot the whole stack and result in a new master election.

Note the following when using the **no stack** <*stack-ID*> **enable** command:

- If the specified `stack-ID` is not used by any current stack member, the command will be rejected.

CAUTION: *Disabling a stack member can significantly degrade the throughput capability of the stack.*

Example To turn on stacking on a stackable stand-alone unit, use the command:

```
awplus# configure terminal
awplus(config)# stack enable
```

Related Commands

reboot

license

stack management subnet

Overview This command configures the subnet address used by the stack management VLAN.

Use the **no** variant of this command to reset the stack's VLAN subnet management address back to the default address and mask (192.168.255.0/27).

Syntax

```
stack management subnet <ip-address>
no stack management subnet
```

Parameter	Description
<ip-address>	The new subnet address for the stack management VLAN.

Default The default stacking management VLAN subnet address is 192.168.255.0 with a subnet mask 255.255.255.224 or /27.

Mode Global Configuration

Usage This command configures the stack management VLAN subnet address.

The management VLAN will be used for high speed communication between stacked units via the stacking ports. Although this command enables you to change the IP address command, the subnet mask must always remain as shown.

The stack management IP subnet is solely used internally to the stacked devices, and cannot be reached external to the stack. You should only change the stack management VLAN subnet address if it causes a conflict within your network.

Note that several separate stacks can use the same default management VLAN subnet address even though their user ports may share the same external network. If the stack subnet address is changed, then the configuration for any new units must also be updated before they are inserted into the stack.

If the management VLAN subnet address is changed by this command, you can use the **no** variant of this command to reset it to its default.

Example To set the management VLAN subnet address to 192.168.255.144:

```
awplus# configure terminal
awplus(config)# stack management subnet 192.168.255.144
```

Related Commands stack management vlan

stack management vlan

Overview Use this command to configure the stack management VLAN ID.

Use the **no** variant of this command to change the stack management VLAN ID back to the default (VLAN ID 4094).

Syntax

```
stack management vlan <2-4094>
no stack management vlan
```

Parameter	Description
<2-4094>	Stack management VLAN ID.

Default VLAN ID 4094

Mode Global Configuration

Usage The management VLAN is used for high speed communication between stacked units. This command enables you to change the ID of this VLAN.

The default stacking management VLAN ID is 4094, which is the last configurable VLAN ID in the switch.

The stack management VLAN is created and configured automatically so that the stack VLAN cannot be used in the stack's VLAN configuration commands (such as`awplus(config-vlan)# vlan <Stack management VLAN ID>`).

The management VLAN should only be changed if the default stack VLAN ID needs to be used in the stack's VLAN configuration.

If the management VLAN ID is changed by this command, you can use the no variant of this command to change it back to default value.

CAUTION: *If the management VLAN ID is changed by this command, you can use the no variant of this command to change it back to the default value.*

When the command is entered, the updated management VLAN configuration will take effect once the stack is restarted.

Examples To set the management VLAN to 4000, enter the following commands:

```
awplus# configure terminal
awplus(config)# stack management vlan 4000
```

To reset the management VLAN back to the default (4094), enter the following commands:

```
awplus# configure terminal
awplus(config)# no stack management vlan
```

Related Commands stack management subnet

stack priority

Overview Use this command to change a specific stack member's master-election priority.

Syntax

```
stack <stack-ID> priority <0-255>
no stack <stack-ID> priority
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.
priority	The stack member's election priority value.
<0-255>	The stack member's new priority value. The lowest value is assigned the highest priority. The default is 128.

Mode Global Configuration

Usage This command is used to change the value of a specific stack member's master-election priority. If the specified `stack-ID` is not used by any current stack member, the command will be rejected.

The election criteria selects the stack member with the lowest priority value to become the stack master. Where two stack members both have the same lowest priority value, then the stack member with the lowest MAC address will be elected as master.

NOTE: *Assigning a new priority value will not immediately change the current stack master. In order to force a master re-election after the new priority value is assigned, use reboot stack-member <master's ID> to reboot the current stack master, a new stack master will then be elected based on the new priority values.*

Example To change the priority of stack member 2 to be 3, use the command:

```
awplus# configure terminal
awplus(config)# stack 2 priority 3
```

Validation Command show stack

stack renumber

Overview Use this command to renumber a specific stack member.

Syntax

```
stack <existing stack-ID> renumber <new stack-ID>
```

Parameter	Description
<existing stack-ID>	We recommend that you use only numbers 1 to 2 for a 2 unit stack, or 1 to 4 for a four unit stack.
`renumber`	Change the existing `stack-ID`.
<new stack-ID>	We recommend that you use only numbers 1 to 2 for a 2 unit stack, or 1 to 4 for a four unit stack.

Default Every stack unit will initially try to use a `stack-ID` of 1.

Mode Global Configuration

Usage This command is used to change the ID of a specific stack member - primarily when exchanging stack members. The changes made by this command will not take effect until the switch is rebooted.

NOTE: *This command does not alter any of the stacks's existing configuration, apart from the `stack-ID` specified. For example, if stack member 2 were removed from the stack and a new stack unit is assigned the member 2 `stack-ID`, then the interface configuration that existed for the removed stack member 2 will be applied to the new stack member 2.*

The existing stack-ID must already be assigned to an existing stack member. To avoid duplicating IDs, a warning message will appear if you assign a new stack-ID that is currently assigned to another stack member. However, you can continue to renumber the stack-IDs and remove ID duplications. If you do not remove the duplications, then one of the devices will be forced to automatically renumber to an unused ID. Once you have removed any duplicate IDs, you can reboot the switch to implement your changes.

Note that the configured `stack-ID` is saved immediately on the renumbered member, and so is not reliant on using the copy running-config command for it to take effect.

Example To renumber stack 1 to stack 2, use the commands:

```
awplus# configure terminal
awplus(config)# stack 1 renumber 2
```

Validation Command show stack

stack renumber cascade

Overview This command is used to renumber the members of a stack so that their IDs are ordered sequentially, relative to the member's physical position within the stack.

CAUTION: Changing the stack numbering will upset the existing stack member configurations such as port settings. This command is intended for use when the stack is either initially commissioned, or has undergone a major reconfiguration. In this situation you run the stack renumber command (which will automatically reboot the switch), then configure the stack members to meet the new requirements.

Syntax

```
stack <stack-ID> renumber cascade [<stack-ID>]
```

Parameter	Description
<stack-ID>	The ID of the stack member to start renumbering from, from 1 to 8.
renumber	Change the existing stack-ID.
cascade	Renumber the existing stack-ID in cascade order.
<stack-ID>	The new ID for the first member renumbered, from 1 to 8 .

Default If no stack-ID is specified, the member will take the default ID of 1.

Mode Global Configuration

Usage This command is used to renumber the members of a stack so that their stack-IDs are ordered sequentially. This would normally be done either when the stack is initially configured or following a major reconfiguration.

The renumber will start on the specified stack member. If that stack-ID is not used by any of the existing stack member, the command will be rejected.

The starting stack member will be renumbered with the new stack-ID specified, or the default of member ID of 1. The stack-ID of the next physically will be the starting members ID +1, for example member ID 2. This renumbering will continue in cascading order around the stack members.

The changes will take place immediately and reboot all stack members. For this reason a confirmation prompt follows this command entry, asking whether you are sure you want to renumber and reboot the entire stack.

Example

```
awplus(config)# stack 1 renumber cascade

Any existing interface configuration
may no longer be valid.
Are you sure you want to renumber and reboot the entire
stack?(y/n): y
```

Related Commands

show stack

switch provision (stack)

stack renumber

stack resiliencylink

Overview This command configures the resiliency link used by the stack. The interface used may be either an eth port or is a dedicated VLAN (resiliencylink VLAN) to which switch ports may become members. This VLAN is dedicated to the resiliency link function and must not be the stack management VLAN.

Syntax

```
stack resiliencylink <interface>
no stack resiliencylink
```

Parameters	Description
<interface>	The name of the interface that is connected to the resiliency link. This may be either the eth port or the resiliencylink VLAN.

Mode Global Configuration

Usage The resiliency-link is only used when a backup member loses connectivity with the master via the stacking cables. Such a communication loss would occur if:

- a stacking link is removed or fails
- two or more stacking link cables are unplugged or fail
- the stack master itself fails due to a reboot or power failure

The resiliency-link allows the backup member to determine if the master is still present in the network by the reception of healthcheck messages sent by the master over the resiliency-link interface.

CAUTION: *The purpose of the resiliency link is to enable the backup master to check the status of the master under fault conditions. If the resiliency link is not configured, and the master loses communication with its other stack member, then the stack will assume the master is NOT present in the network, which could cause network conflicts if the master is still online. Note that this is different to stacking operation in releases prior to version 5.3.1.*

Reply healthcheck messages are received if the master is still online, but the stack will now split into two different "stubs". The stub containing the existing master will continue operating as normal. The members in the masterless stub will now use a "type stack disabled-master" trigger to run a configuration to form a second temporary stack. This utilizes the remaining stack members' resources without conflicting directly with the master's configuration. If no "type stack disabled-master" trigger was configured on the switches, then the masterless stub members will disable their switch ports.

If no healthcheck messages are received, then the master is assumed to be completely offline, and so the other stack members can safely take over the master's configuration.

CAUTION: *The purpose of the resiliency link is to enable the stack members (particularly the backup master) to check the status of the master under fault conditions. If the resiliency link is not configured, and the master loses communication with its other*

stack members, then the stack will assume the master is NOT present in the network, which could cause network conflicts if the master is still online. Note that this is a change to the stacking of releases prior to version 5.3.1.

Example To set the resiliency link to be VLAN 4093.

First use the **stack resiliencylink** command to create the resiliency `vlan 4093`

```
awplus# configure terminal
awplus(config)# stack resiliencylink vlan4093
```

Next use the switchport resiliencylink command to assign the resiliencylink vlan to the interface port, in this case `port1.0.1`.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport resiliencylink
```

Related Commands

show stack

switch provision (stack)

show stack resiliencylink

stack disabled-master-monitoring

switchport resiliencylink

stack software-auto-synchronize

Overview This command re-enables the software version auto-synchronization feature either on a specified stack member or all stack members.

Use the **no** variant of this command to turn the software version auto synchronization feature off.

Syntax

```
stack {all|<stack-ID>} software-auto-synchronize
no stack {all|<stack-ID>} software-auto-synchronize
```

Parameter	Description
`all`	All stack members.
`<stack-ID>`	Stack member number, from 1 to 8.

Default All the stack members have the stack software-auto-synchronize feature enabled by default.

Mode Global Configuration

Usage This command is used to enable the software version auto-synchronization feature for either a specific stack member or all stack members and candidates.

Note that if a device attempts to join a stack but is running a software release that is different to the other stack members, the software version auto-synchronization feature will copy the master's software release onto the new member. If the software version auto- synchronization feature is not enabled, then the device will be unable to join the stack.

Note that the software version auto-synchronization feature may also result in the stack member downgrading its software release if the master is running an older software version.

Examples To turn on the software-auto-synchronize feature on stack member 2, which was previously turned off, use the following commands:

```
awplus# configure terminal
awplus(config# stack 2 software-auto-synchronize
```

To turn on the software-auto-synchronize feature for all stack members, which were previously turned off, use the following commands:

```
awplus# configure terminal
awplus(config)# stack all software-auto-synchronize
```

Validation Command show stack

stack virtual-chassis-id

Overview This command specifies the stack virtual chassis ID. The ID selected will determine which virtual MAC address the stack will use. The MAC address assigned to a stack must be unique within its network.

NOTE: *The command will not take effect until the switch has been rebooted.*

Syntax

```
stack virtual-chassis-id <id>
```

Parameter	Description
<id>	The value of the ID - enter a number in the range 0 to 4095.

Mode Global Configuration

Usage The virtual-chassis-id entered will form the last 12 bits of a pre-selected MAC prefix component; that is, `0000.cd37.0xxx`. If you enable the stack virtual MAC address feature (by using the stack virtual-mac command) without using the stack virtual- chassis-id command to select the virtual-chassis-id, then the stack will select a virtual- chassis-id from a number within the assigned range.

Example To set the stack virtual-chassis-id to 63 use the commands

```
awplus# configure terminal
awplus(config)# stack virtual-chassis-id 63
```

This will result in a virtual MAC address of: `0000.cd37.003f`.

Related Commands

show running-config

show stack

switch provision (stack)

stack virtual-mac

stack virtual-mac

Overview This command enables the stack virtual MAC address feature. For more information on this topic, see the VCStack Feature Overview and Configuration Guide. With this command set, the value applied for the virtual MAC address is determined by the setting of the command stack virtual-chassis-id command.

CAUTION: Stack operation is only supported ifstack virtual-macis enabled.

Before enabling the virtual MAC address feature, you should check that the stack's virtual-chassis-id is not already used by another stack in the network. Otherwise the duplicate MAC addresses will cause problems for the network traffic.

Syntax

```
stack virtual-mac
no stack virtual mac
```

Mode Global Configuration

Usage Note that this command will not take effect until the switch has been rebooted.

Example

```
awplus# configure terminal
awplus(config)# stack virtual mac
```

Related Commands

show running-config

show stack

switch provision (stack)

stack virtual-chassis-id

switch provision (stack)

Overview This command enables you to provide the configuration for a new stack member switch prior to physically connecting it to the stack. To run this command, the stack position must be vacant. The selected hardware type must be compatible existing stack hardware.

Use the **no** variant of this command to remove an existing switch provision.

Syntax

```
switch <stack-ID> provision IX5-28
no switch <stack-ID> provision
```

Parameter	Description
<stack-ID>	Stack member number, from 1 to 8.
provision	Provides settings within the stack configuration ready for a specific switch type to become a stack member.
IX5	Provision a 28-port IX5 switch.

Mode Global Configuration

Usage Note that although the syntax appears to allow provisioning on up to 8 stackable switches, in practice a maximum of 4 are configurable. Normally the stack members would be numbered 1 to 4, and so the command could be run to provision any stack member within this range; and we advise this procedure. In effect, the syntax then becomes:

```
switch <1-4> provision IX5-28
```

However, you could number the stack units with any numbers between 1 and 8. For example you could number your four stack members 1, 2, 7 and 8. In this case you could provision any of the stack members within this range. We advise against numbering your stacks in this way.

Examples To provision an IX5-28 switch as stack member 3, use the following commands:

```
awplus# configure terminal
awplus(config)# switch 3 provision IX5-28
```

To remove the provision of the IX5-28 switch as stack member 3, use the following commands:

```
awplus# configure terminal
awplus(config)# no switch 3 provision
```

switchport resiliencylink

Overview This command configures the switch port to be a member of the stack resiliency link VLAN. Note that this switchport will only be used for stack resiliency-link traffic and will not perform any other function, or carry any other traffic.

The **no** variant of this command removes the switchport from the resiliency link VLAN.

Syntax

```
switchport resiliencylink
no switchport resiliencylink
```

Mode Interface Configuration

Usage Note that a resiliency link cannot be part of a static or dynamic aggregator group.

Examples To set the resiliency link to be VLAN 4093:

First, use the **stack resiliencylink** command to create the resiliency-link vlan `vlan4093`

```
awplus# configure terminal
awplus(config)# stack resiliencylink vlan4093
```

Next, use the **switchport resiliencylink** command to assign the resiliency-link vlan to the port, in this case `port1.0.1`.

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# switchport resiliencylink
```

Related Commands stack resiliencylink

show stack resiliencylink

vlan mode stack-local-vlan

Overview This command enables you to create stack-local-VLANs and use ICMP to monitor and diagnose issues within specific members of the stack. When a VLAN is added using this method, all its traffic will be trapped to and processed by the CPU of the specific local stack member, rather than the CPU of the stack master.

Syntax

```
vlan <vid> mode stack-local-vlan <member-id>
no vlan <vid>
```

Parameter	Description
<vid>	The VID of the VLAN to be created in the range 2-4094. We recommend that the first stack-local-vlan be assigned the number 4001 for the first stack member, then incremented by one for each stack member. For example, a stack of four members would be assigned the following VID numbers: • stack member one: VID 4001 • stack member two: VID 4002 • stack member three: VID 4003 • stack member four: VID 4004
`mode stack-local-vlan`	Specifies that the new VLAN will function as a stack-local-VLAN.
<member-id>	Specifies the new stack member ID. Enter a decimal number in the range 1-8.

Default By default, VLANs are automatically enabled as they are added.

Mode VLAN Configuration

Usage If IGMP snooping is operating on a stack-local-VLAN, the device will try to process some multicast traffic via that VLAN, if it is connected to a Microsoft Windows PC.

To avoid this, we recommend disabling IGMP snooping on stack-local-VLANs, by using the command **no** ip igmp snooping.

Examples To add a stack-local-VLAN with the VID of 4002 and assign it to stack member 2, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan 4002 mode stack-local-vlan 2
awplus(config-vlan)# exit
awplus(config)# interface vlan4002
awplus(config-if)# no ip igmp snooping
```

To remove VLAN 4002, use the following commands:

```
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan 4002
```

Related Commands

ip igmp snooping

mtu

vlan database

undebug stack

Overview This command applies the functionality of the **no** debug stack command.

38 VRRP Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure the Virtual Router Redundancy Protocol (VRRP). For more information, see the VRRP Feature Overview and Configuration Guide.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

advertisement-interval

Overview Use this command to configure the advertisement interval of the virtual router. This is the length of time, in seconds, between each advertisement sent from the master to its backup(s).

IPv6 VRRP advertisements are sent to the multicast address assigned to the VRRP group (ff02:0:0:0:0) and a backup virtual router has to join all multicast groups within this range. VRRP advertisements are sent to a multicast address (ff02::12) every second by default.

Use the **no** variant of this command to remove an advertisement interval of the virtual router, which has been set using the **advertisement-interval** command, and revert to the default advertisement interval of 1 second.

Syntax

```
advertisement-interval [<1-255>|csec <1-4095>]
no advertisement-interval
```

Parameter	Description
<1-255>	Specifies the advertisement interval in seconds.
csec	Use centiseconds instead of seconds for the advertisement interval.
<1-4095>	Specifies the advertisement interval in centiseconds.

Default The default advertisement interval is 1 second.

Mode Router Configuration

Usage Note when using VRRP with VCStacking, ensure the VRRP advertisement-interval is larger than the VCStacking failover time to avoid VCStacking failovers causing VRRP failovers.

See the VRRP Feature Overview and Configuration Guide for more information about:

- setting the advertisement-interval when configuring VRRP
- using seconds for VRRPv2 host compatibility whenever you use transition-mode to upgrade or transition from VRRPv2 to VRRPv3
- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details

NOTE:

When using VRRPv3 with VCStacking, ensure that the VRRPv3 advertisement- interval is configured to a longer time than the VCStacking failover time.

If the VRRPv3 advertisement-interval is shorter than the VCStacking failover time, then a VRRPv3 failover will also occur whenever a VCStacking failover occurs. Use seconds not centiseconds to ensure interoperability with VRRPv2.

Examples

The example below shows you how to configure the advertisement interval to 6 seconds for the VRRP IPv4 session with VR ID 5 on interface vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# advertisement-interval 6
```

The example below shows you how to reset the advertisement interval to the default of 1 second for the VRRP IPv4 session with VR ID 5 on interface vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# no advertisement-interval
```

The example below shows you how to configure the advertisement interval to 6 seconds for the VRRPv3 IPv6 session with VR ID 5 on interface vlan2:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 5 vlan2
awplus(config-router)# advertisement-interval 6
```

Related Commands

router vrrp (interface)

router ipv6 vrrp (interface)

circuit-failover

Overview Use this command to enable the VRRP circuit failover feature.

Circuit failover enables the device to take action if the uplink interface goes down, so that the VRRP backup, whose uplink interface is still active, takes over as VRRP master. See the VRRP Feature Overview and Configuration Guide for more information.

You can use the circuit failover feature to monitor up to 32 interfaces per VRRP instance.

Use the **no** variant of this command to disable this feature.

Syntax

```
circuit-failover <interface> <1-253>
no circuit-failover [<interface> <1-253>]
```

Parameter	Description
<interface>	The interface of the router that is monitored. Interface must exist on the router, and is usually an upstream interface. Should the interface go down, then another router that is configured as a backup router in the group takes over as the master. You should configure the circuit failover on an interface other than the active VRRP interface - generally the uplink interface.
<1-253>	Delta value. The value by which virtual routers decrement their priority value during a circuit failover event. Configure this value to be greater than the difference of priorities on the master and backup routers. In the case of failover, this priority delta value is subtracted from the current VR Master Router priority value.

Mode Router Configuration

Examples To configure circuit failover on an IPv4 VRRP instance, so that if interface VLAN3 goes down, then the priority of VRRP instance 1 is reduced by 30, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 vlan2
awplus(config-router)# circuit-failover vlan3 30
```

To remove all configured circuit failovers for the VRRP IPv4 session with VR ID 1 on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 1 vlan2
awplus(config-router)# no circuit-failover
```

To configure circuit failover on a VRRPv3 IPv6 session with VR ID 1, so that when interface VLAN3 goes down, the priority of VRRP instance 1is reduced by 30, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 1 vlan2
awplus(config-router)# circuit-failover vlan3 30
```

To remove all configured circuit failovers for the VRRPv3 IPv6 session with VR ID 1 on interface vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 1 vlan2
awplus(config-router)# no circuit-failover
```

Related Commands

router vrrp (interface)

router ipv6 vrrp (interface)

debug vrrp

Overview Use this command to specify debugging options for VRRP. The **all** parameter turns on all the debugging options.

Use the **no** variant of this command to disable this function.

Syntax

```
debug vrrp [all]
no debug vrrp [all]
```

Mode Privileged Exec and Global Configuration

Usage See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Examples The example below shows you how to enable all debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp all
```

The example below shows you how to disable all debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp all
```

Related Commands show debugging vrrp

undebug vrrp

debug vrrp events

Overview Use this command to specify debugging options for VRRP event troubleshooting.

Use the **no** variant of this command to disable this function.

Syntax

```
debug vrrp events
no debug vrrp events
```

Mode Privileged Exec and Global Configuration

Usage The **debug vrrp events** command enables the display of debug information related to VRRP internal events.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Examples The example below shows you how to enable events debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp events
```

The example below shows you how to disable events debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp events
```

Related Commands

show debugging vrrp

undebug vrrp events

debug vrrp packet

Overview Use this command to specify debugging options for VRRP packets.

Use the **no** variant of this command to disable this function.

Syntax

```
debug vrrp packet [send|recv]
no debug vrrp packet [send|recv]
```

Parameter	Description
`send`	Specifies the debug option set for sent packets.
`recv`	Specifies the debug option set for received packets.

Mode Privileged Exec and Global Configuration

Usage The **debug vrrp packet** command enables the display of debug information related to the sending and receiving of packets.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Examples The example below shows you how to enable received and sent packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet
```

The example below shows you how to enable only received packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet recv
```

The example below shows you how to enable only sent packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# debug vrrp packet send
```

The example below shows you how to disable packet debugging for VRRP:

```
awplus# configure terminal
awplus(config)# no debug vrrp packet
```

Related Commands show debugging vrrp

undebug vrrp packet

disable (VRRP)

Overview Use this command to disable a VRRP IPv4 session or a VRRPv3 IPv6 session on the router to stop it participating in virtual routing. Note that when this command is configured then a backup router assumes the role of master router depending on its priority. See the enable (VRRP) command to enable a VRRP IPv4 session or a VRRPv3 IPv6 session on the router.

Syntax

```
disable
```

Mode Router Configuration

Usage See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 and IPv6 configuration details.

Examples The example below shows you how to disable the VRRP session for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# disable
```

The example below shows you how to disable the VRRPv3 session for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# disable
```

Related Commands

enable (VRRP)

router vrrp (interface)

router ipv6 vrrp (interface)

show vrrp

enable (VRRP)

Overview Use this command to enable the VRRP session on the router to make it participate in virtual routing. To make changes to the VRRP configuration, first disable the router from participating in virtual routing using the disable (VRRP) command.

Syntax

```
enable
```

Mode Router Configuration

Usage You must configure the virtual IP address and define the interface for the VRRP session (using the virtual-ip or virtual-ipv6 and the router vrrp (interface) or router ipv6 vrrp (interface) commands) before using this command.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 and IPv6 configuration details.

Examples To enable the VRRP session for VRRP VR ID 5 on vlan2, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# enable
```

To enable the VRRPv3 session for VRRPv3 VR ID 3 on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# enable
```

Related Commands

disable (VRRP)

router vrrp (interface)

router ipv6 vrrp (interface)

show vrrp

virtual-ip

virtual-ipv6

preempt-mode

Overview Use this command to configure preempt mode. If preempt-mode is set to **true**, then the highest priority backup will always be the master when the default master is unavailable.

If preempt-mode is set to **false**, then a higher priority backup will not preempt a lower priority backup who is acting as master.

Syntax

```
preempt-mode {true|false}
```

Parameter	Description
`true`	Preemption is enabled.
`false`	Preemption is disabled.

Default The default is **true**.

Mode Router Configuration

Usage When the master router fails, the backup routers come online in priority order—highest to lowest. Preempt mode means that a higher priority back up router will take over the master role from a lower priority back up. Preempt mode on **true** allows a higher priority backup router to relieve a lower priority backup router.

By default, a preemptive scheme is enabled whereby a higher priority backup virtual router that becomes available take over for the backup virtual router that was elected to become the master virtual router.

This preemptive scheme can be disabled using the **preempt-mode false** command. If preemption is disabled, the backup virtual router that is currently elected as the master virtual router does not transition to backup virtual router again whenever the alternate backup router with a higher priority becomes available.

See the VRRP Feature Overview and Configuration Guide for more information about:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- preempt mode

Examples The example below shows you how to configure preempt-mode as true for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# preempt-mode true
```

The example below shows you how to configure preempt-mode as false for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# preempt-mode false
```

The example below shows you how to configure preempt-mode as true for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# preempt-mode true
```

The example below shows you how to configure preempt-mode as false for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# preempt-mode false
```

Related Commands

circuit-failover

priority

router vrrp (interface)

router ipv6 vrrp (interface)

priority

Overview Use this command to configure the VRRP router priority within the virtual router. The highest priority router is Master (unless preempt-mode is false).

Use the **no** variant of this command to remove the VRRP router priority within the virtual router, which has been set using the **priority** command.

Syntax

```
priority <1-255>
no priority
```

Parameter	Description
<1-255>	The priority. For the master router, use 255 for this parameter; otherwise use any number from the range <1-254>.

Default Defaults for priority are: **master router**= 255; **backup**= 100.

Mode Router Configuration

Usage Priority determines the role that each VRRP router plays and what happens if the master virtual router fails. If a VRRP router owns the IP address of the virtual router and the IP address of the interface, then this VRRP router functions as the master virtual router.

Priority also determines whether a VRRP router functions as a backup virtual router and the order of ascendancy to becoming a master virtual router if the master virtual router fails. Configure the priority of each backup virtual router with a a value of 1 through 254.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 and IPv6 configuration details.

Examples The example below shows you how to configure 101 as the priority for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# priority 101
```

The example below shows you how to remove the priority configured for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# no priority
```

The example below shows you how to configure 101 as the priority for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# priority 101
```

The example below shows you how to remove the configured priority for VRRPv3 VR ID 3 on vlan1:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# no priority
```

Related Commands

circuit-failover

preempt-mode

router ipv6 vrrp (interface)

Overview Use this command to configure VRRPv3 for IPv6 and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode.

Use the **no** variant of this command to remove the VRRPv3 for IPv6 configuration. Disable the VRRP session before using the **no** variant of this command.

Syntax

```
router ipv6 vrrp <vrid> <interface>
no router ipv6 vrrp <vrid> <interface>
```

Parameter	Description
<vrid>	*<1-255>* The ID of the virtual router VRRPv3 IPv6 session to create.
<interface>	Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRPv3 IPv6 advertisement messages.

Mode Global Configuration

Usage Use the required *<interface>* placeholder to define the interface that will participate in virtual routing. This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when in master state.

You can configure up to 255 IPv4 and 255 IPv6 VRRP instances. However, configuring a high number of instances may adversely affect the device's performance, depending on the device CPU, the other protocols it is running, and whether you set the advertisement interval to less than 1 second.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Examples The example below shows you how to enable a VRRPv3 session with VR ID 3 on vlan2:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan2
awplus(config-router)# enable
awplus(config-router)#
```

The example below shows you how to disable a VRRPv3 session with VR ID 3 on vlan2:

```
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router ipv6 vrrp 3 vlan2
awplus(config)#
```

Related Commands

advertisement-interval

circuit-failover

router vrrp (interface)

Overview Use this command to configure VRRP IPv4 and define the interface that will participate in virtual routing to send and receive advertisement messages. This command allows you to enter the Router Configuration mode.

Use the **no** variant of this command to remove the VRRP IPv4 configuration. Disable the VRRP session before using the **no** variant of this command.

Syntax

```
router vrrp <vrid> <interface>
no router vrrp <vrid> <interface>
```

Parameter	Description
<vrid>	*<1-255>* The ID of the virtual router VRRP IPv4 session to create.
<interface>	Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRP IPv4 advertisement messages.

Mode Global Configuration

Usage Use the required *<interface>* placeholder to define the interface that will participate in virtual routing. This interface is used for two purposes - to send/receive advertisement messages and to forward on behalf of the virtual router when in master state.

You can configure up to 255 IPv4 and 255 IPv6 VRRP instances. However, configuring a high number of instances may adversely affect the device's performance, depending on the device CPU, the other protocols it is running, and whether you set the advertisement interval to less than 1 second.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Examples To enable a VRRP session with VR ID 5 on vlan1, use the commands:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan1
awplus(config-router)# enable
```

To disable a VRRP session with VR ID 5 on vlan1, use the commands:

```
awplus(config-router)# disable
awplus(config-router)# exit
awplus(config)# no router vrrp 5 vlan1
```

Related Commands

advertisement-interval

circuit-failover

disable (VRRP)

enable (VRRP)

show debugging vrrp

Overview Use this command to display the set VRRP debugging option. Use the terminal monitor command to display output on the console otherwise debug output is in the log file.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 debugging details.

Syntax

```
show debugging vrrp
```

Mode User Exec and Privileged Exec

Example The example below shows you how to display VRRP debugging:

```
awplus# show debugging vrrp
```

Related Commands

debug vrrp

debug vrrp events

debug vrrp packet

show running-config router ipv6 vrrp

Overview Use this command to show the running configuration for VRRPv3 IPv6.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Syntax

```
show running-config router vrrp
```

Mode Privileged Exec, Global Configuration, Line Configuration, and Interface Configuration.

Example The example below shows you how to display the running configuration for VRRPv3 IPv6:

```
awplus# show running-config router ipv6 vrrp
```

Output Figure 38-1: Example output from the **show running-config router ipv6 vrrp** command

```
!
router ipv6 vrrp 3 vlan3
 virtual-ip fe80::202:b3ff:fed5:983e master
 circuit-failover vlan3 3
 advertisement-interval 6
 preempt-mode false
!
```

show running-config router vrrp

Overview Use this command to show the running configuration for VRRP IPv4.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Syntax

```
show running-config router vrrp
```

Mode Privileged Exec, Global Configuration, Line Configuration, and Interface Configuration.

Example The example below shows you how to display the running configuration for VRRP IPv4:

```
awplus# show running-config router vrrp
```

Output Figure 38-2: Example output from the **show running-config router vrrp** command

```
!
router vrrp 2 vlan2
 circuit-failover vlan2 2
 advertisement-interval 4
 preempt-mode true
!
```

show vrrp

Overview Use this command to display information about all VRRP IPv4 sessions. This command shows a summary when the optional **brief** parameter is used.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Syntax

```
show vrrp [brief]
```

Parameter	Description
brief	Brief summary of VRRP sessions.

Mode User Exec and Privileged Exec

Example To display information about all VRRP IPv4 sessions, enter the command:

```
awplus# show vrrp
```

To display brief summary output about VRRP IPv4 sessions, enter the command:

```
awplus# show vrrp brief
```

Output Figure 38-3: Example output from the **show vrrp** command

```
awplus#show vrrp
VMAC enabled
Address family IPv4
VRRP Id: 1 on interface: vlan2
 State: AdminUp    - Master
 Virtual IP address: 192.168.1.2 (Not-owner)
 Priority is 100
 Advertisement interval: 100 centiseconds
 Preempt mode: TRUE
 Multicast membership on IPv4 interface vlan2: JOINED
 Transition mode: FALSE
 Accept mode: FALSE
 Master address: 192.168.1.3
```

Figure 38-4: Example output from the **show vrrp brief** command

```
awplus#show vrrp brief
Interface        Grp  Prio Own  Pre  State      Master addr      Group addr
 vlan10            1   200   N    P  Master     192.168.10.4     192.168.10.253
 vlan10            2   150   N    P  Backup     192.168.10.4     192.168.10.254
 vlan11            3   200   N    P  Master     192.168.11.4     192.168.11.253
 vlan11            4   150   N    P  Backup     192.168.11.4     192.168.11.254
```

Related Commands

enable (VRRP)

disable (VRRP)

show vrrp counters

Overview This command displays VRRP SNMP counters on the console, as described in the VRRP MIB and RFC2787, for debugging use while you configure VRRP with commands in this chapter.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show vrrp counters
```

Mode User Exec and Privileged Exec

Usage The output has a section for global counters and a section of counters for each VRRP instance configured. See the descriptions of the counters below the sample output as per RFC2787.

NOTE: *Note that the counters displayed with this commands are the same counters as described in RFC 2787 (Copyright (C) The Internet Society (2000). All Rights Reserved) except for the "Monitored Circuit Up" and "Monitored Circuit Down" counters, which are additions beyond the MIB.*

Example To display information about VRRP SNMP counters on the console, enter the command:

```
awplus# show vrrp counters
```

Figure 38-5: Example output from the **show vrrp counters** command

```
awplus#show vrrp counters
VRRP Global Counters:
  Checksum Errors .... 230
  Version Errors ..... 0
  VRID Errors ........ 230

VRRP IPv4 counters for VR 10/vlan10:
  Master Transitions ........ 0
  Received Advertisements ... 0
  Internal Errors ........... 0
  TTL Errors ................ 0
  Received Priority 0 Pkt ... 0
  Sent Priority 0 Pkt ....... 0
  Received Invalid Type ..... 0
  Address List Errors ....... 0
  Packet Length Errors ...... 0
  Monitored Circuit Up ...... 0
  Monitored Circuit Down..... 0
```

```
VRRP IPv4 counters for VR 100/vlan100:
  Master Transitions ........ 1
  Received Advertisements ... 1614
  Internal Errors ........... 0
  TTL Errors ................ 0
  Received Priority 0 Pkt ... 0
  Sent Priority 0 Pkt ....... 0
  Received Invalid Type ..... 0
  Address List Errors ....... 0
  Packet Length Errors ...... 0
  Monitored Circuit Up ...... 0
  Monitored Circuit Down..... 2
```

Table 1: Global counters with descriptions for the **show vrrp counters** command:

Counter	Description
`Checksum Errors`	The total number of VRRP packets received with an invalid VRRP checksum value.
`Version Errors`	The total number of VRRP packets received with an unknown or unsupported version number.
`VRID Errors`	The total number of VRRP packets received with an invalid VRID for this virtual router.

Table 2: Per VR counters with descriptions for the **show vrrp counters** command:

Counter	Description
`Master Transitions`	The total number of times that this virtual router's state has transitioned to MASTER.
`Received Advertisements`	The total number of VRRP advertisements received by this virtual router.
`Internal Errors`	The total number of VRRP advertisement packets received for which the advertisement interval is different than the one configured for the local virtual router.
`TTL Errors`	The total number of VRRP packets received by the virtual router with IP TTL (Time-To-Live) not equal to 255.
`Received Priority 0 Pkt`	The total number of VRRP packets received by the virtual router with a priority of '`0`'.
`Sent Priority 0 Pkt`	The total number of VRRP packets sent by the virtual router with a priority of '`0`'.
`Received Invalid Type`	The number of VRRP packets received by the virtual router with an invalid value in the '`type`' field.
`Address List Errors`	The total number of packets received for which the address list does not match the locally configured list for the virtual router.

Table 2: Per VR counters with descriptions for the **show vrrp counters** command: (cont.)

Counter	Description
`Packet Length Errors`	The total number of packets received with a packet length less than the length of the VRRP header.
`Monitored Circuit Up`	The total number of times the monitored circuit has generated the UP event.
`Monitored Circuit Down`	The total number of times the monitored circuit has generated the down event.

show vrrp ipv6

Overview Use this command to display information about all configured VRRPv3 IPv6 sessions for all interfaces, or all VRRPv3 IPv6 sessions for a given interface with the optional parameter.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Syntax

```
show vrrp ipv6 [<interface>]
```

Parameter	Description
<interface>	Specify the name of the interface that will participate in the virtual routing. The interface must exist on the router. The interface specified sends and receives VRRPv3 IPv6 advertisement messages.

Mode User Exec and Privileged Exec

Example To display information about all VRRPv3 IPv6 sessions, enter the command:

```
awplus# show vrrp ipv6
```

Output Figure 38-6: Example output from the **show vrrp ipv6 vlan2** command

```
awplus#show vrrp ipv6 vlan2
VrId <1>
 State is Master
 Virtual IP is fe80::202:b3ff:fed5:983e (Owner)
 Interface is vlan2
 Priority is 255
 Advertisement interval is 4 sec
 Preempt mode is FALSE
```

Related Commands enable (VRRP)

disable (VRRP)

show vrrp (session)

Overview Use this command to display information for a particular VRRP session.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Syntax `show vrrp <vrid> <interface>`

Parameter	Description
<vrid>	*<1-255>* The virtual router ID for which to display information. Session must already exist.
<interface>	The interface to display information about, for instance, `vlan2`.

Mode User Exec and Privileged Exec

Usage See the below sample output from the **show vrrp** command displaying information about VRRP session 1 configured on **vlan2**. Output shows that a Virtual IP address has been set.

```
awplus# show vrrp 1 vlan2
```

```
awplus#show vrrp 1 vlan2
Address family IPv4
VrId <1>
 Interface is vlan2
 State is Initialize
 Virtual IP address is 10.10.11.250 (Not IP owner)
 Priority is 100
 Advertisement interval is 1 sec
```

See the below sample output from the **show vrrp** command displaying information about VRRP session 1 configured on **vlan3**. Output shows a Virtual IP address has not been set.

```
awplus# show vrrp 1 vlan3
```

```
awplus#show vrrp 1 vlan3
Address family IPv4
VrId <1>
 Interface is vlan3
 State is Initialize
 Virtual IP address is unset
 Priority is 100
 Advertisement interval is 1 sec
 Preempt mode is TRUE
```

Example The following command shows information about VRRP session 5 for interface **vlan2**.

```
awplus# show vrrp 5 vlan2
```

transition-mode

Overview Use this command to configure the IPv4 transition mode. Transition mode allows you to upgrade from VRRPv2 to VRRPv3 and gives interoperability between VRRPv2 and VRRPv3.

If transition-mode is set to **true**, then the IPv4 transition mode is enabled and VRRPv2 and VRRPv3 advertisements are sent allowing VRRPv2 and VRRPv3 interoperability. Received VRRPv2 advertisement packets are accepted and processed when transition-mode is true.

If transition-mode is set to **false**, then the IPv4 transition mode is disabled and only VRRPv3 advertisements are sent. Received VRRPv2 advertisement packets are dropped.

Note the advertisement-interval should not be configured to less than 1 second when using transition-mode. VRRPv2 can only use advertisements in whole second intervals.

Syntax

```
transition-mode {true|false}
```

Parameter	Description
`true`	Transition mode is enabled. This results in VRRPv2 and VRRPv3 IPv4 advertisements being sent. Transition mode is only available on VRRPv3 for interoperability with VRRPv2 while upgrading to VRRPv3.
`false`	Transition mode is disabled. This stops VRRPv2 IPv4 advertisements being sent. Only VRRPv3 advertisements are sent when disabled. Disable transition-mode after upgrading from VRRPv2 to VRRPv3.

Default The default is **false**.

Mode Router Configuration

Usage See the VRRP Feature Overview and Configuration Guide for more information:

- VRRPv3 IPv4 configuration details
- VRRPv3 IPv6 configuration details
- further information about configuring transition mode to upgrade from VRRPv2 to VRRPv3

Examples The example below shows you how to configure IPv4 transition-mode as true for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# transition-mode true
```

The example below shows you how to configure IPv4 transition-mode as false for VRRP VR ID 5 on vlan2:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# transition-mode false
```

Related Commands router vrrp (interface)

undebug vrrp

Overview Use this command to disable all VRRP debugging.

Syntax

```
undebug vrrp all
```

Mode Privileged Exec

Example The example below shows you how to disable all VRRP debugging:

```
awplus# undebug vrrp all
```

Related Commands debug vrrp

undebug vrrp events

Overview Use this command to disable debugging options for VRRP event troubleshooting.

Syntax

```
undebug vrrp events
```

Mode Privileged Exec

Example The example below shows you how to disable VRRP event debugging:

```
awplus# undebug vrrp events
```

Related Commands debug vrrp events

undebug vrrp packet

Overview Use this command to disable debugging options for VRRP packets.

Syntax

```
undebug vrrp packet [send|recv]
```

Parameter	Description
`send`	Disable the debug option set for sent packets.
`recv`	Disable the debug option set for received packets.

Mode Privileged Exec

Examples The example below shows you how to disable VRRP sent packet debugging:

```
awplus# undebug vrrp packet send
```

The example below shows you how to disable VRRP received packet debugging:

```
awplus# undebug vrrp packet recv
```

The example below shows you how to disable all VRRP packet debugging:

```
awplus# undebug vrrp packet
```

Related Commands debug vrrp packet

virtual-ip

Overview Use this command to set the virtual IP address for the VRRP session. This is the IP address of the virtual router that end hosts set as their default gateway.

Use the **no** variant of this command to disable this feature.

Syntax

```
virtual-ip <ip-address> [master|backup|owner]
no virtual-ip
```

Parameter	Description
<ip-address>	The virtual IPv4 address of the virtual router, entered in dotted decimal format A.B.C.D.
`master`	Sets the default state of the VRRP router within the Virtual Router as **master**. For master, the router must own the Virtual IP address. Specify the **owner** option before using **master** option.
`backup`	Sets the default state of the VRRP router within the Virtual Router as **backup**.
`owner`	Sets the IPv6 address of the VRRP router within the Virtual Router as the **owner**. Specify this before using the **master** option.

Mode Router Configuration

Usage The VRRP master and owner of the virtual IPv4 address for the VRRP session only responds to the packets destined to the virtual IPv6 address. The VRRP master that is not an owner of the virtual IPv4 address for the VRRP session does not respond to the packets destined to the virtual IPv4 address, but forwards packets with a VMAC as the destination address. See the vrrp vmac command to enable and disable this feature.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv4 configuration details.

Examples The example below shows you how to set the virtual IP address for VRRP VR ID 5 and the router as the VRRP master:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# virtual-ip 192.0.2.30 master
```

The example below shows you how to set the virtual IPv4 address for VRRP VR ID 5 and the router as the VRRP backup:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# virtual-ip 192.0.2.30 backup
```

The example below shows you how to set the virtual IPv4 address for VRRP VR ID 5 and the router as owner of the virtual IPv4 address:

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# virtual-ip 192.0.2.30 owner
```

The example below shows you how to disable the virtual IPv4 address for VRRP VR ID 5

```
awplus# configure terminal
awplus(config)# router vrrp 5 vlan2
awplus(config-router)# no virtual-ip
```

Related Commands

router vrrp (interface)

enable (VRRP)

vrrp vmac

virtual-ipv6

Overview Use this command to set the virtual IPv6 address for the VRRPv3 session. This is the IPv6 address of the virtual router that end hosts set as their default gateway.

Note that the primary IPv6 address specified is an IPv6 link-local address. See the Usage note below for further information.

Use the **no** variant of this command to disable this feature.

Syntax

```
virtual-ipv6 <ipv6-address> [master|backup]
[primary|secondary]
```

```
no virtual-ipv6
```

Parameter	Description
<ipv6-address>	The IPv6 address of the virtual router, entered in hexadecimal, in the format X:X::X.X.
`master`	Sets **master** to be the default state of the VRRPv3 router within the Virtual Router. For **master**, we recommend using a Virtual IP address that is not owned by any of the VRRP routers in the same grouping (that share the same VRID).
`backup`	Sets **backup** to be the default state of the VRRPv3 router within the Virtual Router.
`primary`	Sets the specified address as the primary IPv6 address. The primary address must be a link-local IPv6 address.
`secondary`	Sets the specified address as the secondary IPv6 address. Normally this would be a globally-routable IPv6 address. This enables you to specify a globally-routable address as the default gateway address for all the hosts on a VLAN.

Mode Router Configuration

Usage The virtual router will reply to ping, telnet, and SSH requests to the virtual IP address. The virtual router will reply even if it does not own the virtual IP address.

The AlliedWare Plus VRRPv3 implementation supports one IPv6 virtual link local address per virtual router ID. Note that in the command examples fe80::1 is an IPv6 link-local address. An IPv6 link-local address is used because IPv6 link-local addresses are used by IPv6 ND (Neighbor Discovery). A host's default route to a router points to the IPv6 link- local address, not a specific global IPv6 address for the router. For the host's traffic to switch over to a backup router, the IPv6 link-local address of the router is used by VRRPv3.

See the VRRP Feature Overview and Configuration Guide for more information about VRRPv3 IPv6 configuration details.

Examples

The example below shows you how to set the virtual IPv6 address for VRRPv3 VR ID 3 and the router as the VRRPv3 master:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# virtual-ipv6 fe80::1 master
```

The example below shows you how to set the virtual IPv6 address for VRRPv3 VR ID 3 and the router as the VRRPv3 backup:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# virtual-ipv6 fe80::1 backup
```

The example below shows you disable the virtual IPv6 address for VRRPv3 VR ID 3:

```
awplus# configure terminal
awplus(config)# router ipv6 vrrp 3 vlan1
awplus(config-router)# no virtual-ipv6
```

Related Commands

router ipv6 vrrp (interface)

enable (VRRP)

vrrp vmac

vrrp vmac

Overview Use this command to enable or disable the VRRP Virtual MAC feature. This feature is used by VRRP to make the hosts use the virtual MAC address as the physical hardware address of their gateway.

A VRRP router master will use the virtual MAC address for any ARP responses associated with the virtual IP address, or any gratuitous ARPs sent on behalf of the virtual IP address.

All VRRP advertisements are sent using this virtual MAC address as the source MAC address.

The virtual MAC address has the form 00:00:5e:00:01:<VRID>, where VRID is the ID of the Virtual Router.

Syntax

```
vrrp vmac {enable|disable}
```

Mode Global Configuration

Examples To enable Virtual MAC enter:

```
awplus# configure terminal
awplus(config)# vrrp vmac enable
```

To disable Virtual MAC enter:

```
awplus# configure terminal
awplus(config)# vrrp vmac disable
```

Related Commands virtual-ip

virtual-ipv6

39 Ethernet Protection Switched Ring (EPSRing™) Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Ethernet Protection Switched Ring (EPSRing™). For more information, see the EPSR Feature Overview and Configuration Guide.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

debug epsr

Overview This command enables EPSR debugging.

The **no** variant of this command disables EPSR debugging.

Syntax

```
debug epsr {info|msg|pkt|state|timer|all}
no debug epsr {info|msg|pkt|state|timer|all}
```

Parameter	Description
`info`	Send general EPSR information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above information from being sent to the console.
`msg`	Send the decoded received and transmitted EPSR packets to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above packets from being sent to the console.
`pkt`	Send the received and transmitted EPSR packets as raw ASCII text to the console. Using this parameter with the **no debug epsr** command will explicitly exclude the above packets from being sent to the console.
`state`	Send EPSR state transitions to the console. Using this parameter with the **no debug epsr** command will explicitly exclude state transitions from being sent to the console.
`timer`	Send EPSR timer information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude timer information from being sent to the console.
`all`	Send all EPSR debugging information to the console. Using this parameter with the **no debug epsr** command will explicitly exclude any debugging information from being sent to the console.

Mode Privileged Exec and Global Configuration

Examples To enable state transition debugging, use the command:

```
awplus# debug epsr state
```

To disable EPSR packet debugging, use the command:

```
awplus# no debug epsr pkt
```

Related Commands undebug epsr

epsr

Overview This command sets the timer values for an EPSR instance. These are only valid for master nodes.

NOTE: *Running your switch as an EPSR master node requires a Premium License.*

Syntax

```
epsr <epsr-instance> {hellotime <1-32767>|failovertime
<2-65535> ringflaptime <0-65535>}
```

```
no epsr <epsr-instance>
```

CAUTION: *Using the "no" variant of this command will remove the specified EPSR instance.*

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`hellotime` *<1-32767>*	The number of seconds between the transmission of health check messages.
`failovertime` *<2-65535>*	The number of seconds that a master waits for a returning health check message before entering the failed state. **The failover time should be greater than twice the hellotime.** This is to force the master node to wait until it detects the absence of two sequential healthcheck messages before entering the failed state.
`ringflaptime` *<0-65535>*	The minimum number of seconds that a master must remain in the failed state.

Mode EPSR Configuration

Examples To set the hellotimer to 5 seconds for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue hellotime 5
```

NOTE: *When stacking is used with EPSR, the EPSR **failovertime** should be at least 5 seconds.*

To delete the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)#
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

epsr configuration

epsr datavlan

epsr state

epsr trap

reboot rolling

show epsr

epsr configuration

Overview Use this command to enter EPSR Configuration mode so that EPSR can be configured.

Syntax

```
epsr configuration
```

Mode Global Configuration

Example To change to EPSR mode, use the command:

```
awplus(config)# epsr configuration
```

Related Commands

epsr mode master controlvlan primary port

epsr

show epsr

epsr datavlan

Overview This command adds a data VLAN or a range of VLAN identifiers to a specified EPSR instance.

The **no** variant of this command removes a data VLAN or data VLAN range from an EPSR instance.

Syntax

```
epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}
no epsr <epsr-instance> datavlan {<vlanid>|<vlanid-range>}
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
datavlan	Adds a data VLAN to be protected by the EPSR instance.
<vlanid>	The VLAN's VID - a number between 1 and 4094 excluding the number selected for the control VLAN.
<vlanid-range>	Specify a range of VLAN identifiers using a hyphen to separate identifiers.

Mode EPSR Configuration

Usage We recommend you

- set the EPSR control VLAN to vlan2, using the epsr mode master controlvlan primary port and epsr mode transit controlvlan commands, then
- set the EPSR data VLAN between to be a value between 3 and 4094, using the epsr datavlan command.

Examples To add `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan3
```

To add `vlan2` and `vlan3` to the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue datavlan vlan2-vlan3
```

To remove `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan3
```

To remove `vlan2` and `vlan3` from the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue datavlan vlan2-vlan3
```

Related Commands epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

epsr enhancedrecovery enable

Overview This command enables EPSR's enhanced recovery mode. Enhanced recovery mode enables a ring to apply additional recovery procedures when a ring with more than one break partially mends. For more information, see the EPSR Feature Overview and Configuration Guide.

The **no** variant of this command disables the enhanced recovery mode.

Syntax

```
epsr <epsr-instance> enhancedrecovery enable
no epsr <epsr-instance> enhancedrecovery enable
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Default Default is that enhanced recovery mode disabled.

Mode EPSR Configuration

Example To apply enhanced recovery on the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue enhancedrecovery enable
```

Related Commands show epsr

epsr mode master controlvlan primary port

Overview This command creates a master EPSR instance.

NOTE: *Running your switch as an EPSR master node requires a Premium License.*

Syntax

```
epsr <epsr-instance> mode master controlvlan <2-4094>
primaryport <port>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`mode`	Determines the node is acting as a master.
`master`	Sets switch to be the master node for the named EPSR ring.
`controlvlan`	The VLAN that will transmit EPSR control frames.
<2-4094>	VLAN id.
`primaryport`	Primary port for the EPSR instance.
<port>	The primary port. The port may be a switch port (e.g. `port1.0.4`) or a static channel group (e.g. `sa2`). It cannot be a dynamic (LACP) channel group.

NOTE:

The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch or stacked node. However, we advise against this because in certain situations it can produce unpredictable results.

Mode EPSR Configuration

Example To create a master EPSR instance called `blue` with `vlan2` as the control VLAN and `port1.0.1` as the primary port, use the command:

```
awplus(config-epsr)# epsr blue mode master controlvlan vlan2
primaryport port1.0.1
```

Related Commands

epsr mode transit controlvlan

show epsr

epsr mode transit controlvlan

Overview This command creates a transit EPSR instance.

Syntax

```
epsr <epsr-instance> mode transit controlvlan <2-4094>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
mode	Determines the node is acting as a transit node.
transit	Sets switch to be the transit node for the named EPSR ring.
controlvlan	The VLAN that will transmit EPSR control frames.
<2-4094>	VLAN id.

NOTE: *The software allows you to configure more than two ports or static channel groups to the control VLAN within a single switch or stacked node. However, we advise against this because in certain situations it can produce unpredictable results.*

If the control VLAN contains more than two ports (or static channels) an algorithm selects the two ports or channels with the lowest number to be the ring ports. However if the switch has only one channel group is defined to the control vlan, EPSR will not operate on the secondary port.

EPSR does not support Dynamic link aggregation (LACP).

Mode EPSR Configuration

Example To create a transit EPSR instance called `blue` with `vlan2` as the control VLAN, use the command:

```
awplus(config-epsr)# epsr blue mode transit controlvlan vlan2
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

epsr priority

Overview This command sets the priority of an EPSR instance on an EPSR node. Priority is used to prevent "superloops" forming under fault conditions with particular ring configurations. Setting a node to have a priority greater than one, also has the effect of turning on **superloop protection**.

The **no** variant of this command returns the priority of the EPSR instance back to its default value of 0, which also disables EPSR Superloop prevention.

Syntax

```
epsr <epsr-instance> priority <0-127>
no <epsr-instance> priority
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`priority`	The priority of the ring instance selected by the epsr-name parameter.
<0-127>	The priority to be applied (0 is the lowest priority and represents no superloop protection).

Default The default priority of an EPSR instance on an EPSR node is 0. The negated form of this command resets the priority of an EPSR instance on an EPSR node to the default value.

Mode EPSR Configuration

Example To set the priority of the EPSR instance called `blue` to the highest priority (127), use the command:

```
awplus(config-epsr)# epsr blue priority 127
```

To reset the priority of the EPSR instance called `blue` to the default (0), use the command:

```
awplus(config-epsr)# no epsr blue priority
```

Related Commands epsr configuration

epsr state

Overview This command enables or disables an EPSR instance.

Syntax

```
epsr <epsr-instance> state {enabled|disabled}
```

Parameter	Description
<epsr-instance>	The name of the EPSR instance.
state	The operational state of the ring.
enabled	EPSR instance is enabled.
disabled	EPSR instance is disabled.

Mode EPSR Configuration

Example To enable the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue state enabled
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

epsr trap

Overview This command enables SNMP traps for an EPSR instance. The traps will be sent when the EPSR instance changes state.

The **no** variant of this command disables SNMP traps for an EPSR instance. The traps will no longer be sent when the EPSR instance changes state.

Syntax

```
epsr <epsr-instance> trap
no epsr <epsr-instance> trap
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.
`trap`	SNMP trap for the EPSR instance.

Mode EPSR Configuration

Example To enable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# epsr blue trap
```

To disable traps for the EPSR instance called `blue`, use the command:

```
awplus(config-epsr)# no epsr blue trap
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

show debugging epsr

Overview This command shows the debugging modes enabled for EPSR.

Syntax

```
show debugging epsr
```

Mode User Exec and Privileged Exec

Example To show the enabled debugging modes, use the command:

```
awplus# show debugging epsr
```

Related Commands debug epsr

show epsr

Overview This command displays information about all EPSR instances.

Syntax

```
show epsr
```

Mode User Exec and Privileged Exec

Example To show the current settings of all EPSR instances, use the command:

```
awplus# show epsr
```

Output: non-superloop topology The following examples show the output display for a non-superloop topology network.

Table 1: Example output from the **show epsr** command run on a transit node

```
EPSR Information
-------------------------------------------------------------
 Name ........................ test2
 Mode ........................ Transit
 Status ...................... Enabled
 State ....................... Links-Up
 Control Vlan ................ 2
 Data VLAN(s) ................ 10
 Interface Mode .............. Ports Only
 First Port .................. port1.0.1
 First Port Status ........... Down
 First Port Direction ........ Unknown
 Second Port ................. port1.0.2
 Second Port Status .......... Down
 Second Port Direction ....... Unknown
 Trap ........................ Enabled
 Master Node ................. Unknown
 Enhanced Recovery ........... Disabled
-------------------------------------------------------------
```

Table 2: Example output from the **show epsr** command run on a master node

```
EPSR Information
-------------------------------------------------------------
 Name ....................... test4
 Mode ........................ Master
 Status ...................... Enabled
 State ....................... Complete
 Control Vlan ................ 4
 Data VLAN(s) ................ 20
 Interface Mode .............. Ports Only
 Primary Port ................ port1.0.3
 Primary Port Status ......... Forwarding
 Secondary Port .............. port1.0.4
 Secondary Port Status ....... Forwarding
 Hello Time .................. 1 s
 Failover Time ............... 2 s
 Ring Flap Time .............. 0 s
 Trap ........................ Enabled
 Enhanced Recovery ........... Disabled
-------------------------------------------------------------
```

NOTE: *The above screen is only viewable when running the switch as an EPSR Master. Running the switch as a master requires a Premium license.*

Output: superloop topology

The following examples show the output display for superloop topology network.

Table 3: Example output from the **show epsr** command run on a Master Node

```
 EPSR Information
-------------------------------------------------------------
 Name ....................... test4
 Mode ........................ Master
 Status ...................... Enabled
 State ....................... Complete
 Control Vlan ................ 4
 Data VLAN(s) ................ 20
 Interface Mode .............. Ports Only
 Primary Port ................ port1.0.3
   Status .................... Forwarding (logically blocking)
   Is On Common Segment ...... No
   Blocking Control .......... Physical
 Secondary Port .............. port1.0.4
   Status .................... Blocked
   Is On Common Segment ...... No
   Blocking Control .......... Physical
 Hello Time .................. 1 s
 Failover Time ............... 2 s
 Ring Flap Time .............. 0 s
 Trap ........................ Enabled
 Enhanced Recovery ........... Disabled
 SLP Priority ................ 12
-------------------------------------------------------------
```

NOTE: *The above screen is only viewable when running the switch as an EPSR Master.*

Running the switch as a master requires a Premium license.

Table 4: Example output from the **show epsr** command run on a Transit Node

```
 EPSR Information
-------------------------------------------------------------
 Name ........................ test4
 Mode ........................ Transit
 Status ...................... Enabled
 State ....................... Complete
 Control Vlan ................ 4
 Data VLAN(s) ................ 20
 Interface Mode .............. Ports Only
 Primary Port ................ port1.0.3
   Status .................... Forwarding (logically blocking)
   Is On Common Segment ...... No
   Blocking Control .......... Physical
 Secondary Port .............. port1.0.4
   Status .................... Blocked
   Is On Common Segment ...... No
   Blocking Control .......... Physical
 Hello Time .................. 1 s
 Failover Time ............... 2 s
 Ring Flap Time .............. 0 s
 Trap ........................ Enabled
 Enhanced Recovery ........... Disabled
 SLP Priority ................ 12
-------------------------------------------------------------
```

Table 5: Parameters displayed in the output of the **show epsr** command

Parameter on Master Node	Parameter on Transit Node	Description
Name	Name	The name of the EPSR instance.
Mode	Mode	The mode in which the EPSR instance is configured - either Master or Transit
Status	Status	Indicates whether the EPSR instance is enabled or disabled
State	State	Indicates state of the EPSR instance's state machine. Master states are: Idle, Complete, and Failed. Transit states are Links-Up, Links-Down, and Pre-Forwarding.
Control Vlan	Control Vlan	Displays the VID of the EPSR instance's control VLAN.
Data VLAN(s)	Data VLAN(s)	The VID(s) of the instance's data VLANs.
Interface Mode	Interface Mode	Whether the EPSR instance's ring ports are both physical ports (Ports Only) or are both static aggregators (Channel Groups Only).
Primary Port	First Port	The EPSR instance's primary ring port.

Table 5: Parameters displayed in the output of the **show epsr** command (cont.)

Parameter on Master Node	Parameter on Transit Node	Description
- Status	- Status	Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port because it does not have physical control of it.
	- Direction	The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"
- Is On Common Segment	- Is On Common Segment	Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment.
- Blocking Control	- Blocking Control	Whether the instance has "physical" or "logical" control of the ring port's blocking in the instance's data VLANs.
Secondary Port	Second Port	The EPSR instance's secondary port.
- Status	- Status	Whether the ring port is forwarding (Forwarding) or blocking (Blocked), or has link down (Down), and if forwarding or blocking, "(logical)" indicates the instance has only logically set the blocking state of the port, because it does not have physical control of it. Note that on a master configured for SuperLoop Prevention (non-zero priority) its secondary ring port can be physically forwarding, but logically blocking. This situation arises when it is not the highest priority node in the topology (and so does not receive LINKS-DOWN messages upon common segment breaks) and a break on a common segment in its ring is preventing reception of its own health messages.
	- Direction	The ring port on which the last EPSR control packet was received is indicated by "Upstream". The other ring port is then "Downstream"
- Is On Common Segment	- Is On Common Segment	Whether the ring port is on a shared common segment link to another node, and if so, "(highest rank)" indicates it is the highest priority instance on that common segment
- Blocking Control	- Blocking Control	Whether the instance has "physical" or "logical" control of the ring port's blocking in the instance's data VLANs
Hello Time		The EPSR instance's setting for the interval between transmissions of health check messages (in seconds)
Failover Time		The time (in seconds) the EPSR instance waits to receive a health check message before it decides the ring is down
Ring Flap Time		The minimum time the EPSR instance must remain in the failed state
Trap	Trap	Whether the EPSR instance has EPSR SNMP traps enabled

Table 5: Parameters displayed in the output of the **show epsr** command (cont.)

Parameter on Master Node	Parameter on Transit Node	Description
`Enhanced Recovery`	`Enhanced Recovery`	Whether the EPSR instance has enhanced recovery mode enabled
`SLP Priority`	`SLP Priority`	The EPSR instance's priority (for SuperLoop Prevention)

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr counters

show epsr common segments

Overview This command displays information about all the superloop common segment ports on the switch.

Syntax

```
show epsr common segments
```

Example To display information about all the superloop common segment ports on the switch, use the command:

```
awplus# show epsr common segments
```

Table 6: Example output from the **show epsr common segments** command

```
EPSR Common Segments

Common Seg  EPSR                          Port     Phys Ctrl  Ring
Ring Port   Instance         Mode     Prio  Type     of Port?   Port Status
-------------------------------------------------------------------------------
port1.0.24  test_inst_Red    Transit  127   Second     Yes      Fwding
            test_inst_Blue   Transit  126   Second     No       Fwding (logical)
            test_inst_Green  Transit  125   First      No       Fwding (logical)

sa4         testA            Master    15   Primary    Yes      Blocking
            testB            Transit   14   Second     No       Fwding (logical)

sa5         test_55          Transit    8   First      Yes      Down
            test_77          Transit    7   First      No       Down
-------------------------------------------------------------------------------
```

Related Commands

show epsr

show epsr summary

show epsr counters

show epsr config-check

Overview This command checks the configuration of a specified EPSR instance, or all EPSR instances.

If an instance is enabled, this command will check for the following errors or warnings:

- The control VLAN has the wrong number of ports.
- There are no data VLANs.
- Some of the data VLANs are not assigned to the ring ports.
- The failover time is less than 5 seconds, for a stacked device.
- The instance is a master that shares a common segment with a higher priority instance.
- The instance is a master that shares a common segment with another master.
- The instance is a master with its secondary port on a common segment.

Syntax

```
show epsr [<instance>] config-check
```

Parameter	Description
<instance>	Name of the EPSR instance to check on.

Mode User Exec and Privileged Exec

Example To check the configuration of all EPSR instances and display the results, use the command:

```
awplus# show epsr config-check
```

Table 7: Example output from the **show epsr** config-check command

```
EPSR             Status   Description
Instance
------------------------------------------------------------------------
red              Warning  Failover time is 2s but should be 5s because
                 device is stacked.
white            OK.
blue             Warning  Primary port is not in data VLANs 29-99.
orange           OK.

Don't forget to check that this node's configuration is consistant with all
other nodes in the ring.
------------------------------------------------------------------------
```

Related Commands show epsr

show epsr <epsr-instance>

Overview This command displays information about the specified EPSR instance.

Syntax

```
show epsr <epsr-instance>
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Mode User Exec and Privileged Exec

Example To show the current settings of the EPSR instance called `blue`, use the command:

```
awplus# show epsr blue
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr counters

show epsr <epsr-instance> counters

Overview This command displays counter information about the specified EPSR instance.

Syntax

```
show epsr <epsr-instance> counters
```

Parameter	Description
<epsr-instance>	Name of the EPSR instance.

Mode User Exec and Privileged Exec

Example To show the counters of the EPSR instance called `blue`, use the command:

```
awplus# show epsr blue counters
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

show epsr counters

Overview This command displays counter information about all EPSR instances.

Syntax

```
show epsr counters
```

Mode User Exec and Privileged Exec

Example To show the counters of all EPSR instances, use the command:

```
awplus# show epsr counters
```

Related Commands

epsr mode master controlvlan primary port

epsr mode transit controlvlan

show epsr

show epsr summary

Overview This command displays summary information about all EPSR instances on the switch

Syntax

```
show epsr summary
```

Mode User Exec and Privileged Exec

Example To display EPSR summary information, use the command:

```
awplus# show epsr summary
```

Table 8: Example output from the **show epsr summary** command

```
EPSR Summary Information

Abbreviations:
  M = Master node
  T = Transit node
  C = is on a common segment with other instances
  P = instance on a common segment has physical control of the shared port's
        data VLAN blocking
  LB = ring port is Logically Blocking - applicable to master only

EPSR                                  Ctrl       Primary/1st     Secondary/2nd
Instance      Mode Status   State     VLAN  Prio Port Status     Port Status
-------------------------------------------------------------------------------
test-12345      T  Enabled  Links-Down    6  127  Blocking (C,P)  Blocking (C,P)
test1           M  Enabled  Complete      5   12  Fwding          Fwding (LB)
test2           T  Enabled  Pre-Fwding    4  126  Fwding (C)      Blocking (C)
localB          T  Disabled Idle         40    0  Unknown         Unknown
localC          T  Disabled Idle         41    0  Unknown         Unknown
-------------------------------------------------------------------------------
```

undebug epsr

Overview This command applies the functionality of the **no** variant of the debug epsr command.

Part 7: Network Management

40 Allied Telesis Management Framework™ (AMF) Commands

Introduction

This chapter provides an alphabetical reference for Allied Telesis Management Framework™ (AMF) commands.

AMF Naming Convention

When AMF is enabled on a device, it will automatically be assigned a host name. If a host name has already been assigned, by using the command hostname on page 224, this will remain. If however, no host name has been assigned, then the name applied will be the prefix, **host**_ followed (without a space) by the MAC address of the device. For example, a device whose MAC address is **0016.76b1.7a5e** will have the name **host_0016_76b1_7a5e** assigned to it.

To efficiently manage your network using AMF, we strongly advise that you devise a naming convention for your network devices, and accordingly apply an appropriate hostname to each device in your AMF network.

Command List

atmf area

Overview This command creates an AMF area and gives it a name and ID number.

Use the **no** variant of this command to remove the AMF area.

This command is only valid on AMF controllers, master nodes and gateway nodes.

Syntax

```
atmf area <area-name> id <1-126> [local]
no atmf area <area-name>
```

Parameter	Description
<area-name>	The AMF area name. The area name can be up to 15 characters long. Valid characters are: a..z A..Z 0..9 - _ Names are case sensitive and must be unique within an AMF network. The name cannot be the word "local" or an abbreviation of the word "local" (such as "l", "lo" etc.).
<1-126>	An ID number that uniquely identifies this area.
`local`	Set the area to be the local area. The local area contains the device you are configuring.

Mode Global Configuration

Usage This command enables you to divide your AMF network into areas. Each area is managed by at least one AMF master node. Each area can have up to 120 nodes, depending on the license installed on that area's master node.

The whole AMF network is managed by up to 8 AMF controllers. Each AMF controller can communicate with multiple areas. The number of areas supported on a controller depends on the license installed on that controller.

You must give each area in an AMF network a unique name and ID number.

Only one local area can be configured on a device. You must specify a local area on each controller, remote AMF master, and gateway node.

Example To create the AMF area named *New-Zealand*, with an ID of 1, and specify that it is the local area, use the command:

```
controller-1(config)# atmf area New-Zealand id 1 local
```

To configure a remote area named *Auckland*, with an ID of 100, use the command:

```
controller-1(config)# atmf area Auckland id 100
```

Related Commands

atmf area password

show atmf area

show atmf area summary

show atmf area nodes

switchport atmf-arealink remote-area

atmf area password

Overview This command sets a password on an AMF area.

Use the **no** variant of this command to remove the password.

This command is only valid on AMF controllers, master nodes and gateway nodes. The area name must have been configured first.

Syntax

```
atmf area <area-name> password [8] <password>
no atmf area <area-name> password
```

Parameter	Description
<area-name>	The AMF area name.
8	This parameter is displayed in **show running-config** output to indicate that it is displaying the password in encrypted form. You should not enter **8** on the CLI yourself.
<password>	The password is between 8 and 32 characters long. It can include spaces.

Mode Global Configuration

Usage You must configure a password on each area that an AMF controller communicates with, except for the controller's local area. The areas must already have been created using the atmf area command.

Enter the password identically on both of:

- the area that locally contains the controller, and
- the remote AMF area masters

The command **show running-config atmf** will display the encrypted version of this password. The encryption keys will match between the controller and the remote AMF master.

If multiple controller and masters exist in an area, they must all have the same area configuration.

Example To give the AMF area named *Auckland* a password of "secure#1" use the following command on the controller:

```
controller-1(config)# atmf area Auckland password secure#1
```

and also use the following command on the master node for the Auckland area:

```
auck-master(config)# atmf area Auckland password secure#1
```

Related Commands

atmf area

show atmf area

show atmf area summary

show atmf area nodes

switchport atmf-arealink remote-area

atmf backup

Overview This command can only be applied to a master node. It manually schedules an AMF backup to start at a specified time and to execute a specified number of times per day.

Use the **no** variant of this command to disable the schedule.

Syntax

```
atmf backup {default|<hh:mm> frequency <1-24>}
```

Parameter	Description
`default`	Restore the default backup schedule.
`<hh:mm>`	Sets the time of day to apply the first backup, in hours and minutes. Note that this parameter uses the 24 hour clock.
`backup`	Enables AMF backup to external media.
`frequency <1-24>`	Sets the number of times within a 24 hour period that backups will be taken.

Default Backups run daily at 03:00 AM, by default

Mode Global Configuration

Usage Running this command only configures the schedule. To enable the schedule, you should then apply the command atmf backup enable.

Example To schedule backup requests to begin at 11 am and execute twice per day (11 am and 11 pm), use the following command:

```
node_1# configure terminal
node_1(config)# atmf backup 11:00 frequency 2
```

CAUTION: *File names that comprise identical text, but with differing case, such as Test.txt and test.txt, will not be recognized as being different on FAT32 based backup media such as a USB storage device. However, these filenames will be recognized as being different on your Linux based device. Therefore, for good practice, ensure that you apply a consistent case structure for your back-up file names.*

Related Commands

atmf backup enable

atmf backup stop

show atmf backup

atmf backup area-masters delete

Overview Use this command to delete from external media, a backup of a specified node in a specified area.

Note that this command can only be run on an AMF controller.

Syntax

```
atmf backup area-masters delete area <area-name> node
<node-name>
```

Parameter	Description
<area-name>	The area that contains the node whose backup will be deleted.
<node-name>	The node whose backup will be deleted.

Mode Privileged Exec

Example To delete the backup of the remote area-master named “well-gate” in the AMF area named Wellington, use the command:

```
controller-1# atmf backup area-masters delete area Wellington
node well-gate
```

Related Commands show atmf backup area

atmf backup area-masters enable

Overview Use this command to enable backup of remote area-masters from the AMF controller. This command is only valid on AMF controllers.

Use the **no** form of the command to stop backups of remote area-masters.

Syntax

```
atmf backup area-masters enable
no atmf backup area-masters enable
```

Mode Global configuration

Default Remote area backups are disabled by default

Usage Use the following commands to configure the remote area-master backups:

- atmf backup to configure when the backups begin and how often they run
- atmf backup server to configure the backup server.

Example To enable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf backup area-masters enable
```

To disable scheduled backups of AMF remote area-masters, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf backup area-masters enable
```

Related Commands

atmf backup server

atmf backup

show atmf backup area

atmf backup area-masters now

Overview Use this command to run an AMF backup of one or more remote area-masters from the AMF controller immediately.

This command is only valid on AMF controllers.

Syntax

```
atmf backup area-masters now [area <area-name>|area <area-name>
node <node-name>]
```

Parameter	Description
<area-name>	The area whose area-masters will be backed up.
<node-name>	The node that will be backed up.

Mode Privileged Exec

Example To back up all local master nodes in all areas controlled by controller-1, use the command

```
controller-1# atmf backup area-masters now
```

To back up all local masters in the AMF area named Wellington, use the command

```
controller-1# atmf backup area-masters now area Wellington
```

To back up the local master “well-master” in the Wellington area, use the command

```
controller-1# atmf backup area-masters now area Wellington node
well-master
```

Related Commands

atmf backup area-masters enable

atmf backup area-masters synchronize

show atmf backup area

atmf backup area-masters synchronize

Overview Use this command to synchronize backed-up area-master files between the active remote file server and the backup remote file server. Files are copied from the active server to the remote server.

Note that this command is only valid on AMF controllers.

Syntax

```
atmf backup area-masters synchronize
```

Mode Privileged Exec

Example To synchronize backed-up files between the remote file servers for all area-masters, use the command:

```
controller-1# atmf backup area-masters synchronize
```

Related Commands

atmf backup area-masters enable

atmf backup area-masters now

show atmf backup area

atmf backup bandwidth

Overview This command sets the maximum bandwidth in kilobytes per second (kBps) available to the AMF backup process. This command enables you to restrict the bandwidth that is utilized for downloading file contents during a backup.

NOTE: *This command will only run on an AMF master. An error message will be generated if the command is attempted on node that is not a master.*

Also note that setting the bandwidth value to zero will allow the transmission of as much bandwidth as is available, which can exceed the maximum configurable speed of 1000 kBps. In effect, zero means unlimited.

Use the **no** variant of this command to reset (to its default value of zero) the maximum bandwidth in kilobytes per second (kBps) available when initiating an AMF backup. A value of zero tells the backup process to transfer files using unlimited bandwidth.

Syntax

```
atmf backup bandwidth <0-1000>
no atmf backup bandwidth
```

Parameter	Description
<0-1000>	Sets the bandwidth in kilobytes per second (kBps)

Default The default value is zero, allowing unlimited bandwidth when executing an AMF backup.

Mode Global Configuration

Examples To set an atmf backup bandwidth of 750 kBps, use the commands:

```
node2# configure terminal
node2(config)# atmf backup bandwidth 750
```

To set the AMF backup bandwidth to the default value for unlimited bandwidth, use the commands:

```
node2# configure terminal
node2(config)# no atmf backup bandwidth
```

Related Commands show atmf backup

atmf backup delete

Overview This command removes the backup file from the external media of a specified AMF node.

Note that this command can only be run from an AMF master node.

Syntax

```
atmf backup delete <node-name>
```

Parameter	Description
<node-name>	The AMF node name of the backup file to be deleted.

Mode Privileged Exec

Example To delete the backup file from node2, use the following command:

```
Node_1# atmf backup delete node2
```

Related Commands

show atmf backup

atmf backup now

atmf backup stop

atmf backup enable

Overview This command enables automatic AMF backups on the AMF master node that you are connected to. By default, automatic backup starts at 3:00 AM. However, this schedule can be changed by the atmf backup command. Note that backups are initiated and stored only on the master nodes.

Use the **no** variant of this command to disable any AMF backups that have been scheduled and previously enabled.

Syntax

```
atmf backup enable
no atmf backup enable
```

Default Automatic AMF backup functionality is enabled on the AMF master when it is configured and external media, i.e. an SD card or a USB storage device or remote server, is detected.

Mode Global Configuration

Usage A warning message will appear if you run the atmf backup enable command with either insufficient or marginal memory availability on your external storage device.

You can use the command show atmf backup on page 1633 to check the amount of space available on your external storage device.

Example To turn on automatic AMF backup, use the following command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup enable
```

Related Commands

show atmf

show atmf backup

atmf backup

atmf backup now

atmf enable

atmf backup guests delete

Overview This command removes a guest node's backup files from external media such as a USB drive, SD card, or an external file server.

Syntax

```
atmf backup guests delete <node-name> <guest-port>
```

Parameter	Description
<node-name>	The name of the guest's parent node.
<guest-port>	The port number on the parent node.

Mode User Exec/Privileged Exec

Example On a parent node named **node1** (which, in this case, the user has a direct console connection to) use the following command to remove the backup files of the guest node that is directly connected to port1.0.3.

```
node1# atmf backup guests delete node1 port1.0.3
```

Related Command

atmf backup delete

atmf backup area-masters delete

show atmf backup guest

atmf backup guests enable

Overview Use this command to enable backups of remote guest nodes from an ATMF master.

Use the **no** variant of this command to disable the ability of the guest nodes to be backed up.

Syntax

```
atmf backup guests enable
no atmf backup guests enable
```

Default Guest node backups are enabled by default.

Mode Global Config

Example On the ATMF master node, enable all scheduled guest node backups:

```
atmf-master# configure terminal
atmf-master(config)# atmf backup guests enable
```

Related Commands

atmf backup area-masters enable

show atmf backup guest

atmf backup guests synchronize

atmf backup guests now

Overview This command manually triggers an AMF backup of guest nodes on a AMF Master.

Syntax

```
atmf backup guests now [<node-name>] [<guest-port>]
```

Parameter	Description
<node-name>	The name of the guest's parent node.
<guest-port>	The port number that connects to the guest node.

Default N/A

Mode Privileged Exec

Example Use the following command to manually trigger the backup of all guests in the AMF network

```
awplus# atmf backup guests now
```

Example To manually trigger the backup of a guest node connected to port 1.0.23 of node1, use the following command:

```
awplus# atmf backup guests now node1 port1.0.23
```

Related Commands show atmf backup guest

atmf backup guests synchronize

Overview This command initiates a manual synchronization of all guest backup file-sets across remote file servers and various redundancy backup media, such as USB storage devices. This facility ensures that each device contains the same backup image files. Note that this backup synchronization process will occur as part of the regular backups scheduled by the atmf backup command.

Syntax
```
atmf backup guests synchronize
```

Default N/A

Mode User Exec/Privileged Exec

Example To synchronize backups across remote file servers and storage devices, use the command:

```
Node1#atmf backup guests synchronize
```

Related Commands
atmf backup redundancy enable

show atmf guest

atmf backup guests enable

atmf backup now

Overview This command initiates an immediate AMF backup of either all AMF members, or a selected AMF member. Note that this backup information is stored in the external media on the master node of the device on which this command is run, even though the selected AMF member may not be a master node.

Note that this command can only be run on an AMF master node.

Syntax

```
atmf backup now [<nodename>]
```

Parameter	Description
<nodename> or *<hostname>*	The name of the AMF member to be backed up, as set by the command hostname on page 224. Where no name has been assigned to this device, then you must use the default name, which is the word "host", then an underscore, then (without a space) the MAC address of the device to be backed up. For example host_0016_76b1_7a5e. Note that the node-name appears as the command Prompt when in Privileged Exec mode.

Default A backup is initiated for all nodes on the AMF (but stored on the master nodes).

Mode Privileged Exec

Usage Although this command will select the AMF node to be backed-up, it can only be run from any AMF master node.

NOTE: *The backup produced will be for the selected node but the backed-up config will reside on the external media of the AMF master node on which the command was run. However, this process will result in the information on one master being more up-to-date. To maintain concurrent backups on both masters, you can apply the backup now command to the master working-set. This is shown in Example 4 below.*

Example 1 In this example, an AMF member has not been assigned a host name. The following command is run on the AMF_Master_2 node to immediately backup the device that is identified by its MAC address of 0016.76b1.7a5e:

```
AMF_Master_2# atmf backup now host_0016_76b1_7a5e
```

NOTE: *When a host name is derived from its MAC address, the syntax format entered changes from XXXX.XXXX.XXXX to XXXX_XXXX_XXXX.*

Example 2 In this example, an AMF member has the host name, **office_annex**. The following command will immediately backup this device:

```
AMF_Master_2# atmf backup now office_annex
```

This command is initiated on the device's master node named **AMF_Master_2** and initiates an immediate backup on the device named **office_annex**.

Example 3 To initiate from AMF_master_1 an immediate backup of all AMF member nodes, use the following command:

```
AMF_Master_1# amf backup now
```

Example 4 To initiate an immediate backup of the node with the host-name “office_annex” and store the configuration on both masters, use the following process:

From the AMF_master_1, set the working-set to comprise only of the automatic group, master nodes.

```
AMF_Master_1# atmf working-set group master
```

This command returns the following display:

```
============================
AMF_Master_1, AMF_Master_2
============================

Working set join
```

Backup the AMF member with the host name, **office_annex** on both the master nodes as defined by the working set.

```
AMF_Master[2]# atmf backup now office_annex
```

Note that the [2] shown in the command prompt indicates a 2 node working-set.

Related Commands

atmf backup

atmf backup stop

hostname

show atmf backup

atmf backup redundancy enable

Overview This command is used to enable or disable AMF backup redundancy.

Syntax

```
atmf backup redundancy enable
no atmf backup redundancy enable
```

Default Disabled

Mode Global Configuration

Usage If the AMF Master or Controller supports any removable media (SD card/USB), it uses the removable media as the redundant backup for the AMF data backup.

This feature is valid only if remote file servers are configured on the AMF Master or Controller.

Example To enable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# atmf backup redundancy enable
```

To disable AMF backup redundancy, use the commands:

```
awplus# configure terminal
awplus(config)# no atmf backup redundancy enable
```

Related Commands

atmf backup synchronize

show atmf backup

show atmf backup area

atmf backup server

Overview This command configures remote file servers as the destination for AMF backups.

Use the **no** variant of this command to remove the destination server(s). When all servers are removed the system will revert to backup from external media.

Syntax

```
atmf backup server id {1|2} <hostlocation> username <username>
[path <path>|port <1-65535>]
```

```
no atmf backup server id {1|2}
```

Parameter	Description
`id`	Remote server backup server identifier.
`{1|2}`	The backup server identifier number (1 or 2). Note that there can be up to two backup servers, numbered 1 and 2 respectively, and you would need to run this command separately for each server.
<hostlocation>	Either the name or the IP address (IPv4 or IPv6) of the selected backup server (1 or 2).
`username`	Configure the username to log in with on the selected remote file server.
<username>	The selected remote file server's username.
`path`	The location of the backup files on the selected remote file server. By default this will be the home directory of the username used to log in with.
<path>	The directory path utilized to store the backup files on the selected remote file server. No spaces are allowed in the path.
`port`	The connection to the selected remote backup file server using SSH. By default SSH connects to a device on TCP port 22 but this can be changed with this command.
`<1-65535>`	A TCP port within the specified range.

Defaults Remote backup servers are not configured. The default SSH TCP port is 22. The path utilized on the remote file server is the home directory of the username.

Mode Global Exec

Usage The hostname and username parameters must both be configured.

Examples To configure server 1 with an IPv4 address and a username of *backup1*, use the commands:

```
AMF_Master_1# configure terminal
```

```
AMF_Master_1(config)# atmf backup server id 1 192.168.1.1
username backup1
```

To configure server 1 with an IPv6 address and a username of *backup1*, use the command:

```
AMF_backup1_1# configure terminal
AMF_Master_1(config)# atmf backup server id 1 FFEE::01 username backup1
```

To configure server 2 with a hostname and username, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com username backup2
```

To configure server 2 with a hostname and username in addition to the optional path and port parameters, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# atmf backup server id 2 www.example.com username backup2 path tokyo port 1024
```

To unconfigure the AMF remote backup file server 1, use the command:

```
AMF_Master_1# configure terminal
AMF_Master_1(config)# no atmf backup server id 1
```

Related Commands show atmf backup

atmf backup stop

Overview Running this command stops a backup that is currently running on the master node you are logged onto. Note that if you have two masters and want to stop both, then you can either run this command separately on each master node, or add both masters to a working set, and issue this command to the working set.

Note that this command can only be run on a master node.

Syntax

```
atmf backup stop
```

Mode Privileged Exec

Usage This command is used to halt an AMF backup that is in progress. In this situation the backup process will finish on its current node and then stop.

Example To stop a backup that is currently executing on master node node-1, use the following command:

```
AMF_Master_1# amf backup stop
```

Related Commands

atmf backup

atmf backup enable

atmf backup now

show atmf backup

atmf backup synchronize

Overview For the master node you are connected to, this command initiates a system backup of files from the node's active remote file server to its backup remote file server. Note that this process happens automatically each time the network is backed up.

Note that this command can only be run from a master node.

Syntax

```
atmf backup synchronize
```

Mode Privileged Exec

Example When connected to the master node AMF_Master_1, the following command will initiate a backup of all system related files from its active remote file server to its backup remote file server.

```
AMF_Master_1# atmf backup synchronize
```

Related Commands

atmf backup enable

atmf backup redundancy enable

show atmf

show atmf backup

atmf cleanup

Overview This command erases all data from NVS and all data from Flash excluding the following:

- The current release file and its /flash/.release file
- The backup release file and /flash/.backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw_v2.lic

It then reboots to put the device in a clean state ready to be used as a replacement node on a provisioned port.

Syntax

```
atmf cleanup
```

Mode Privileged Exec

Usage This command is an alias to the erase factory-default command.

Example To erase data, use the command:

```
Node_1# atmf cleanup
This command will erase all NVS, all flash contents except for
the boot release, and any license files, and then reboot the
switch. Continue? (y/n):y
```

Related Commands erase factory-default

atmf controller

Overview Use this command to configure the device as an AMF controller. This enables you to split a large AMF network into multiple areas.

The number of areas supported on a controller depends on the license installed on that controller.

Syntax

```
atmf controller
no atmf controller
```

Mode Global configuration

Usage A valid AMF license must be available before this command can be applied.

Example To configure the node named *controller-1* as an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# atmf controller
```

To stop the node named *controller-1* from being an AMF controller, use the commands:

```
controller-1# configure terminal
controller-1(config)# no atmf controller
```

Related Commands atmf area

show atmf

atmf distribute firmware

Overview This command can be used to upgrade software one AMF node at a time. A URL can be selected from any media location. The latest compatible release for a node will be selected from this location.

Several procedures are performed to ensure the upgrade will succeed. This includes checking the current node release boots from flash. If there is enough space on flash the software release is copied to flash on the new location.

The new release name is updated using the boot system command. The old release will become the backup release file. If a release file exists in a remote device (such as TFTP or HTTP, for example) then the URL should specify the exact release filename without using a wild card character.

The command will continue to upgrade software until all nodes are upgraded. At the end of the upgrade cycle the command should be used on the working-set.

Syntax `atmf distribute firmware <filename>`

Parameter	Description
<filename>	The filename and path of the file. See the File Management Feature Overview and Configuration Guide for valid syntax.

Mode Privileged Exec

Examples To upgrade nodes in a AMF network with a predefined AMF group called sw_team, use the following commands:

```
SW_Team1# atmf working-set group sw_team
```

```
============================
SW_Team1, SW_Team2, SW_Team3:
============================
Working set join
```

```
ATMF_NETWORK[3]# atmf distribute firmware card:*.rel
```

```
Retrieving data from SW_Team1
Retrieving data from SW_Team2
Retrieving data from SW_Team3

ATMF Firmware Upgrade:

Node Name          New Release File           Status
-----------------------------------------------------------------
SW_Team1           x510-main-20140204-2.rel   Release ready
SW_Team2           x610-main-20140204-2.rel   Release ready
SW_Team3           x610-main-20140204-2.rel   Release ready
Continue the rolling reboot ? (y/n):y
=================================================================
Copying Release    : x510-main-20140204-2.rel to SW_Team1
Updating Release   : x510-main-20140204-2.rel information on SW_Team1
=================================================================
Copying Release    : x610-main-20140204-2.rel to SW_Team2
Updating Release   : x610-main-20140204-2.rel information on SW_Team2
=================================================================
Copying Release    : x610-main-20140204-2.rel to SW_Team3
Updating Release   : x610-main-20140204-2.rel information on SW_Team3

=================================================================
New firmware will not take effect until nodes are rebooted.
=================================================================

ATMF_NETWORK[3]#
```

Related Commands atmf working-set

atmf domain vlan

Overview The AMF domain VLAN is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANS (the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

When an AMF network is first created all its nodes are assigned a domain VLAN with a default (domain) VID of 4091. An important point conceptually is that although this VLAN then exists globally across the AMF network, it is assigned separately to each domain. The AMF network therefore can be thought of as comprising a series of domain VLANS each having the same VID and each being applied to a horizontal slice (domain) of the AMF. It follows therefore that the domain VLANs are only applied to ports that form cross-links and not to ports that form uplinks/downlinks.

If you assign a VLAN ID to this VLAN (i.e. changing its value from the default of 4091) then you will need to do this separately on every device within the AMF network. The AMF domain subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

Use the **no** variant of this command to reset the VLAN ID to its default value of 4091.

Syntax

```
atmf domain vlan <2-4090>
no atmf domain vlan
```

Parameter	Description
<2-4090>	The VLAN number in the range 2 to 4090.

Default The default domain VLAN ID for the AMF is 4091.

Mode Global Configuration

Usage The VLANs involved in this process must be reserved for AMF and cannot be used for other purposes. This command enables you to change the domain VLAN to match your network's specific configuration.

CAUTION: *Setting this command, then rebooting the device, will only apply the AMF VLAN for the device being configured. The new domain VLAN will not become effective for the AMF network until all its member nodes have been updated, and all its member devices rebooted.*

As part of its automatic creation process, this VLAN will also be assigned an IP subnet address based on the value configured by the command atmf management subnet on page 1571. Refer to this command for more information.

Examples To change the AMF domain VLAN to 4000 use the following commands:

```
node-1# configure terminal
node-1(config)# atmf domain vlan 4000
```

To reset the AMF domain VLAN to its default of 4091, use the following commands:

```
node-1# configure terminal
node-1(config)# no atmf domain vlan
```

atmf enable

Overview This command manually enables (turns on) the AMF feature for the device being configured.

Use the **no** variant of this command to disable (turn off) the AMF feature on the member node.

Syntax

```
atmf enable
no atmf enable
```

Default Once AMF is configured, the AMF feature starts automatically when the device starts up.

Mode Global Configuration

Usage The device does not auto negotiate AMF domain specific settings such as the Network Name. You should therefore, configure your device with any domain specific (non default) settings before enabling AMF.

Examples To turn off AMF, use the command:

```
MyNode# config terminal
MyNode(config)# no atmf enable
```

To turn on AMF, use the command:

```
MyNode(config)# atmf enable
```

This command returns the following display:

```
% Warning: The ATMF network config has been set to enable
% Save the config and restart the system for this change to take
effect.
```

atmf group (membership)

Overview This command configures a device to be a member of one or more AMF groups. Groups exist in three forms: Implicit Groups, Automatic Groups, and User-defined Groups.

- Implicit Groups
  - all: All nodes in the AMF
  - current: The current working-set
  - local: The originating node.

Note that the Implicit Groups do not appear in show group output.

- Automatic Groups - These are defined by hardware architecture, e.g. x510, x610, x8100, AR3050S, AR4050S.
- User-defined Groups - These enable you to define arbitrary groups of AMF members based on your own criteria.

Each node in the AMF is automatically assigned membership to the implicit groups, and the automatic groups that are appropriate to its node type, e.g. x610, PoE. Similarly, nodes that are configured as masters are automatically assigned to the master group.

Use the **no** variant of this command to remove the membership.

Syntax

```
atmf group <group-list>
no atmf group <group-list>
```

Parameter	Description
<group-list>	A list of group names. These should be entered as a comma delimited list without spaces.

Mode Global Configuration

Usage You can use this command to define your own arbitrary groups of AMF members based on your own network's configuration requirements. Applying a node to a non existing group will result in the group automatically being created.

Note that the master nodes are automatically assigned to be members of the pre-existing master group.

The following example configures the device to be members of three groups; two are company departments, and one comprises all devices located in building_2. To avoid having to run this command separately on each device that is to be added to these groups, you can remotely assign all of these devices to a working-set, then use the capabilities of the working-set to apply the atmf group (membership) command to all members of the working set.

Example 1 To specify the device to become a member of AMF groups named *marketing*, *sales*, and *building_2*, use the following commands:

```
node-1# configure terminal
node-1(config)# atmf group marketing,sales,building_2
```

Example 2 To add the nodes *member_node_1* and *member_node_2* to groups *building1* and *sales*, first add the nodes to the working-set:

```
master_node# atmf working-set member_node_1,member_node_2
```

This command returns the following output confirming that the nodes *member_node_1* and *member_node_2* are now part of the working-set:

```
============================
member_node_1, member_node_2
============================

Working set join
```

Then add the members of the working set to the groups:

```
atmf-net[2]# configure terminal
atmf-net[2](config)# atmf group building1,sales
atmf-net[2](config)# exit
atmf-net[2]# show atmf group
```

This command returns the following output displaying the groups that are members of the working-set.

```
====================
member_node_1
====================

AMF group information

building1, sales
```

Related Commands

show atmf group

show atmf group members

atmf guest-class

Overview This modal command creates a guest-class. Guest-classes are modal templates that can be applied to selected guest types. Once you have created a guest-class, you can select it by entering its mode. From here, you can then configure a further set of operational settings specifically for the new guest-class. These settings can then all be applied to a guest link by running the switchport atmf-guestlink command. The following settings can be configured from each guest class mode:

- discovery method
- model type
- http-enable setting
- guest port, user name, and password

The **no** variant of this command removes the guest-class. Note that you cannot remove a guest-class that is assigned to a port.

Syntax

```
atmf guest-class <guest-class-name>
no atmf guest-class
```

Parameter	Description
<guest-class-name>	The name assigned to the guest-class type. This can be chosen from an arbitrary string of up to 15 characters.

Mode Interface

Example 1 To create a guest-class named **camera** use the following commands:

```
node1# configure terminal
node1(config)# atmf guest-class camera
node1(config-atmf-guest)# end
```

Example 2 To remove the guest-class named **phone** use the following commands:

```
node1# configure terminal
node1(config)# no atmf guest-class phone
node1(config-atmf-guest)# end
```

Related Commands

show atmf area guests

discovery

http-enable

username

modeltype

switchport atmf-guestlink

atmf log-verbose

Overview This command limits the number of log messages displayed on the console or permanently logged.

Syntax

```
atmf log-verbose <1-3>
no atmf log-verbose
```

Parameter	Description
<1-3>	The verbose limitation (3 = noisiest, 1 = quietest)

Default The default log display is 3.

Usage This command is intended for use in large networks where verbose output can make the console unusable for periods of time while nodes are joining and leaving.

Mode Global Configuration

Example To set the log-verbose to noise level 2, use the command:

```
node-1# configure terminal
node-1(config)# atmf log-verbose 2
```

Validation Command show atmf

atmf management subnet

Overview This command is used to assign a subnet that will be allocated to the AMF management and domain management VLANs. From the address space defined by this command, two subnets are created, a management subnet component and a domain component, as explained in the Usage section of this command description.

AMF uses these internal IPv4 subnets when exchanging its inter nodal status packets. These subnet addresses must be reserved for AMF and should be used for no other purpose.

The new management subnet will not become effective until all members of the AMF network have been updated and all its units rebooted.

Use the **no** variant of this command to remove the assigned subnet VLANs.

Syntax

```
atmf management subnet <a.b.0.0>
no atmf management subnet
```

Parameter	Description
<a.b.0.0>	The IP address selected for the management subnet. Because a mask of 255.255.0.0 (i.e. /16) will be applied automatically, an IP address in the format a.b.0.0 must be selected. Usually this subnet address is selected from an appropriate range from within the private address space of 172.16.0.0 to 172.31.255.255, or 192.168.0.0 as defined in RFC1918.

Default 172.31.0.0. Asubnet mask of 255.255.0.0 will automatically be applied.

Mode Global Configuration

Usage Typically a network administrator would use this command to change the default subnet address to match local network requirements.

As previously mentioned, running this command will result in the creation of a further two subnets (within the class B address space assigned) and the mask will extend from /16 to /17.

For example, if the management subnet is assigned the address 172.31.0.0/16, this will result in the automatic creation of the following two subnets:

- 172.31.0.0/17 assigned to the atmf management vlan
- 172.31.128.0/17 assigned to the atmf domain vlan.

Examples To change the AMF management subnet address on node node-1 to 172.25.0.0:

```
node-1# configure terminal
node-1(config)# atmf management subnet 172.25.0.0
```

To change the AMF management subnet address on node node-1 back to its default of 172.31.0.0:

```
node-1# configure terminal
node-1(config)# no atmf management subnet
```

atmf management vlan

Overview The AMF management VLAN is created when the AMF network is first initiated and is assigned its default VID of 4092. This command enables you to change the VID from this default value.

The AMF management vlan is one of the internal VLANs that are used to communicate information about the state of the AMF network between nodes. AMF uses its internal VLANS (such as the management VLAN and the domain VLAN) to communicate its inter nodal network status information. These VLANs must be reserved for AMF and not used for other purposes.

If you assign a VLAN ID to this VLAN (i.e. change its value from the default of 4092) then you will need to do this separately on every device within the AMF. The AMF management subnet will then be applied to this new VID when all devices within the AMF network are next rebooted.

Use the **no** variant of this command to restore the VID to the default of 4092.

Syntax

```
atmf management vlan <2-4090>
no atmf management vlan
```

Parameter	Description
<2-4090>	The VID assigned tro the AMF management VLAN.

Default VLAN ID default is 4092

NOTE: *Although the value applied by default lies outside the user configurable range. You can use the "no" variant of this command to reset the VLAN to its default value.*

mode Global Configuration

Usage You can use this command to change the management VLAN to meet your network's requirements and standards, particularly in situations where the default address value is unacceptable.

NOTE: *This VLAN will automatically be assigned an IP subnet address based on the value configured by the command atmf management subnet. Refer to this command description for further details.*

Examples To change the AMF management VLAN to 4090 use the following commands:

```
VCF-1# configure terminal
VCF-1(config)# atmf management vlan 4090
```

To reset the AMF domain VLAN to its default of 4092, use the following commands:

```
VCF-1# configure terminal
VCF-1(config)# no atmf management vlan 4090
```

atmf master

Overview This command configures the device to be an AMF master node and automatically creates an AMF master group. The master node is considered to be the core of the AMF network, and must be present for the AMF to form. The AMF master has its node depth set to 0. Note that the node depth vertical distance is determined by the number of uplinks/downlinks that exist between the node and its master.

An AMF master node must be present for an AMF network to form. Up to two AMF master nodes may exist in a network, and they **must** be connected by an AMF crosslink.

NOTE: *Master nodes are an essential component of an AMF network. In order to run AMF, an AMF License is required for each master node.*

If the crosslink between two AMF masters fails, then one of the masters will become isolated from the rest of the AMF network.

Use the **no** variant of this command to remove the device as an AMF master node. The node will retain its node depth of 0 until the network is rebooted.

NOTE: *Node depth is the vertical distance (or level) from the master node (whose depth value is 0).*

Syntax

```
atmf master
no atmf master
```

Default The device is not configured to be an AMF master node.

Mode Global Configuration

Example To specify that this node is an AMF master, use the following command:

```
node-1# configure terminal
node-1(config)# atmf master
```

Related Commands show atmf

show atmf group

atmf mtu

Overview This command configures the ATMF network Maximum Transmission Unit (MTU). The MTU value will be applied to the ATMF Management VLAN, the ATMF Domain VLAN and ATMF Area links.

Use the **no** variant of this command to restore the default MTU.

Syntax

```
atmf mtu <1300-1442>
no atmf mtu
```

Parameter	Description
<1300-1442>	The value of the maximum transmission unit for the AMF network, which sets the maximum size of all ATMF packets generated from the device.

Default 1300

Mode Global Configuration

Usage The default value of 1300 will work for all AMF networks (including those that involve virtual links over IPsec tunnels). If there are virtual links over IPsec tunnels anywhere in the AMF network, we recommend not changing this default. If there are no virtual links over IPsec tunnels, then this AMF MTU value may be increased for network efficiency.

Example To change the ATMF network MTU to 1442, use the command:

```
awplus(config)# atmf mtu 1442
```

Related Commands show atmf detail

atmf network-name

Overview This command applies an AMF network name to a (prospective) AMF node. In order for an AMF network to be valid, its network-name must be configured on at least two nodes, one of which must be configured as a master and have an AMF License applied. These nodes may be connected using either AMF downlinks or crosslinks.

For more information on configuring an AMF master node, see atmf master.

Use the **no** variant of this command to remove the AMF network name.

Syntax

```
atmf network-name <name>
no atmf network-name
```

Parameter	Description
<name>	The AMF network name. Up to 15 printable characters can be entered for the network-name.

Mode Global Configuration

Usage This is one of the essential commands when configuring AMF and must be entered on each node that is to be part of the AMF. This command will not take effect until the particular node is rebooted.

A switching node (master or member) may be a member of only one AMF network.

CAUTION: *Ensure that you enter the correct network name. Entering an incorrect name will cause the AMF network to fragment (at the next reboot).*

Example To set the AMF network name to amf_net use the command:

```
Node_1(config)# atmf network-name amf_net
```

atmf node-recovery disable-forwarding

Overview [PSh-Sept2012- This command has been assigned the status of "Developer Only." It is NOT to appear in any User or Technical Support document.

atmf provision

Overview This command configures a specified port on an AMF node to accept a provisioned node, via an AMF link, some time in the future.

Use the **no** variant of this command to remove the provisioning on the node.

Syntax

```
atmf provision [<nodename>]
no atmf provision
```

Parameter	Description
<nodename>	The name of the provisioned node that will appear on the AMF network in the future.

Default No AMF provisioning.

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage The port should be configured as an AMF link or cross link and should be “down” to add or remove a provisioned node.

Example To provision an AMF node named node1 for port1.0.1, use the command:

```
host1(config)# interface port1.0.1
host1(config-if)# atmf provision node1
```

Related Commands

switchport atmf-link

switchport atmf-crosslink

show atmf links

atmf provision node clone

Overview This command sets up a space on the backup media for use with a provisioned node and copies into it almost all files and directories from a chosen backup or provisioned node.

Alternatively, you can set up a new, unique provisioned node by using the command atmf provision node create.

Syntax `atmf provision node <nodename> clone <source-nodename>`

Parameter	Description
<nodename>	The name that will be assigned to the clone when connected.
<source-nodename>	The name of the node whose configuration is to be copied for loading to the clone.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network.

You must run either this command or atmf provision node create command, before you can use other **atmf provision node** commands using the specified node name. If a backup or provisioned node already exists for the specified node then you must delete it before using the **atmf provision node clone** command.

When using this command it is important to be aware of the following:

- A copy of <*media*>:atmf/<*atmf_name*>/nodes/<*source_node*>/flash will be made for the provisioned node and stored in the backup media.
- The directory <*node_backup_dir*>/flash/.config/ssh is excluded from the copy.
- All contents of <*root_backup_dir*>/nodes/<*nodename*> will be deleted or overwritten.
- Settings for the expected location of other provisioned nodes are excluded from the copy.

The active and backup configuration files are automatically modified in the following ways:

- The **hostname** command is modified to match the name of the provisioned node.
- The **stack virtual-chassis-id** command is removed, if present.

Example To copy from the backup of device2 to create backup files for the new provisioned node device3 use the following command:

```
device1# atmf provision node device3 clone device2
```

Figure 40-1: Sample output from the **atmf provision node clone** command

```
device1#atmf provision node device3 clone device2
Copying...
Successful operation
```

To confirm that a new provisioned node has been cloned, use the command:

```
device1# show atmf backup
```

The output from this command is shown in the following figure, and shows the details of the new provisioned node device3.

Figure 40-2: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 .................. Unconfigured
   2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
device3       -            -         No       Yes       Prov
device1       01 Jan 2014  00:05:49  No       Yes       Good
device2       01 Jan 2014  00:05:44  Yes      Yes       Good
```

atmf provision node configure boot config

Overview This command sets the configuration file to use during the next boot cycle. This command can also set a backup configuration file to use if the main configuration file cannot be accessed for an AMF provisioned node. To unset the boot configuration or the backup boot configuration use the **no boot** command.

Use the **no** variant of this command to set back to the default.

Syntax

```
atmf provision node <nodename> configure boot config [backup]
[<file-path|URL>]
```

```
atmf provision node [<nodename>] configure no boot config
[backup]
```

Parameter	Description
<nodename>	The name of the provisioned node.
<file-path|URL>	The path or URL and name of the configuration file.

Default No boot configuration files or backup configuration files are specified for the provisioned node.

Mode Privileged Exec

Usage When using this command to set a backup configuration file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples To set the configuration file `branch.cfg` on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot config
branch.cfg
```

To set the configuration file `backup.cfg` as the backup to the main configuration file on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot config
backup usb:/atmf/amf_net/nodes/node1/config/backup.cfg
```

To unset the boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
config
```

To unset the backup boot configuration, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
config backup
```

Related Commands atmf provision node configure boot system

show atmf provision nodes

atmf provision node configure boot system

Overview This command sets the release file that will load onto a specified provisioned node during the next boot cycle. This command can also set the backup release file to be loaded for an AMF provisioned node. To unset the boot system release file or the backup boot release file use the **no boot** command.

Use the **no** variant of this command to set back to the default.

This command can only be run on AMF master nodes.

Syntax

```
atmf provision node <nodename> configure boot system [backup]
[<file-path|URL>]
```

```
atmf provision node <nodename> configure no boot system [backup]
```

Parameter	Description
<nodename>	The name of the provisioned node.
<file-path|URL>	The path or URL and name of the release file.

Default No boot release file or backup release files are specified for the provisioned node.

Mode Privileged Exec

Usage When using this command to set a backup release file, the specified AMF provisioned node must exist. The specified file must exist in the flash directory created for the provisioned node in the AMF remote backup media.

Examples To set the release file `x610-5.4.4-1.rel` on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot system
x610-5.4.4-1.rel
```

To set the backup release file `x610-5.4.4-1.rel` as the backup to the main release file on the AMF provisioned node `node1`, use the command:

```
MasterNodeName# atmf provision node node1 configure boot system
backup card:/atmf/amf_net/nodes/node1/flash/x610-5.4.4-1.rel
```

To unset the boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
system
```

To unset the backup boot release, use the command:

```
MasterNodeName# atmf provision node node1 configure no boot
system backup
```

Related Commands atmf provision node configure boot config

show atmf provision nodes

atmf provision node create

Overview This command sets up an empty directory on the backup media for use with a provisioned node. This directory can have configuration and release files copied to it from existing devices. Alternatively, the configuration files can be created by the user.

An alternative way to create a new provisioned node is with the command atmf provision node clone.

This command can only run on AMF master nodes.

Syntax

```
atmf provision node <nodename> create
```

Parameter	Description
<nodename>	The name of the node that is being provisioned.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network.

The atmf provision node create command (or atmf provision node clone) must be executed before you can use other **atmf provision node** commands with the specified node name. If a backup or provisioned node already exists for the specified node name then you must delete it before using this command.

A date and time is assigned to the new provisioning directory reflecting when this command was executed. If there is a backup or provisioned node with the same name on another AMF master then the most recent one will be used.

Example To create a new provisioned node named device2 use the command:

```
device1# atmf provision node device2 create
```

Running this command will create the following directories:

- <*media*>:atmf/<*atmf_name*>/nodes/<*node*>
- <*media*>:atmf/<*atmf_name*>/nodes/<*node*>/flash

To confirm the new node's settings, use the command:

```
device1# show atmf backup
```

The output for the **show atmf backup** command is shown in the following figure, and shows details for the new provisioned node device2.

Figure 40-3: Sample output from the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 02 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7315.2MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 .................. Unconfigured
   2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
device2       -            -         No       Yes       Prov
device1       01 Jan 2014  00:05:49  No       Yes       Good
```

For instructions on how to configure on a provisioned node, see the AMF Feature Overview and Configuration Guide.

Related commands

atmf provision node clone

atmf provision node delete

Overview This command deletes files that have been created for loading onto a provisioned node. It can only be run on master nodes.

Syntax

```
atmf provision node <nodename> delete
```

Parameter	Description
<nodename>	The name of the provisioned node to be deleted.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up (although the device itself is still yet to be installed). Otherwise, an error message is shown when the command is run.

You may want to use the **atmf provision node delete** command to delete a provisioned node that was created in error or that is no longer needed.

This command cannot be used to delete backups created by the AMF backup procedure. In this case, use the command atmf backup delete to delete the files.

NOTE: *This command allows provisioned entries to be deleted even if they have been referenced by the atmf provision command, so take care to only delete unwanted entries.*

Example To delete backup files for a provisioned node named device3 use the command:

```
device1# atmf provision node device3 delete
```

To confirm that the backup files for provisioned node device3 have been deleted use the command:

```
device1# show atmf backup
```

The output should show that the provisioned node device3 no longer exists in the backup file, as shown in the figure below:

Figure 40-4: Sample output showing the **show atmf backup** command

```
device1#show atmf backup

Scheduled Backup ...... Enabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 01 Jan 2014 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... USB (Total 7446.0MB, Free 7297.0MB)
Server Config .........
  Synchronization ..... Unsynchronized
    Last Run .......... -
   1 .................. Unconfigured
   2 .................. Unconfigured
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

-----------------------------------------------------------------
Node Name     Date         Time      In ATMF  On Media  Status
-----------------------------------------------------------------
device1       01 Jan 2014  00:05:49  No       Yes       Good
device2       01 Jan 2014  00:05:44  Yes      Yes       Good
```

Related commands atmf provision node create

atmf provision node license-cert

Overview This command is used to set up the license certificate for a provisioned node.

The certificate file usually has all the license details for the network, and can be stored anywhere in the network. This command makes a hidden copy of the certificate file and stores it in the space set up for the provisioned node on AMF backup media.

For node provisioning, the new device has not yet been part of the AMF network, so the user is unlikely to know its product ID or its MAC address. When such a device joins the network, assuming that this command has been applied successfully, the copy of the certificate file will be applied automatically to the provisioned node.

Once the new device has been resurrected on the network and the certificate file has been downloaded to the provisioned node, the hidden copy of the certificate file is deleted from AMF backup media.

Use the **no** variant of this command to set it back to the default.

This command can only be run on AMF master nodes.

Syntax

```
atmf provision node <nodename> license-cert <file-path|URL>
no atmf provision node <nodename> license-cert
```

Parameter	Description
<nodename>	The name of the provisioned node.
<file-path|URL>	The name of the certificate file. This can include the file-path of the file.

Default No license certificate file is specified for the provisioned node.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network. It will only operate if the provisioned node specified in the command has already been set up, and if the license certification is present in the backup file. Otherwise, an error message is shown when the command is run.

Example 1 To apply the license certificate cert1.txt stored on a TFTP server for AMF provisioned node *device2*, use the command:

```
device1# atmf provision node device2 license-cert
tftp://192.168.1.1/cert1.txt
```

Example 2 To apply the license certificate cert2.txt stored in the AMF master's flash directory for AMF provisioned node *host2*, use the command:

```
device1# atmf provision node host2 license-cert /cert2.txt
```

To confirm that the license certificate has been applied to the provisioned node, use the command show atmf provision nodes. The output from this command is shown below, and displays license certification details in the last line.

Figure 40-5: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .............: SD (Total 3827.0MB, Free 3481.1MB)

Node Name                 : device2
Date & Time               : 06-May-2014 & 23:25:44
Provision Path            : card:/atmf/nodes

Boot configuration :
Current boot image        : x510-1766_atmf_backup.rel (file exists)
Backup  boot image        : x510-main-20140113-2.rel (file exists)
Default boot config       : flash:/default.cfg (file exists)
Current boot config       : flash:/abc.cfg (file exists)
Backup  boot config       : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file           : ./.configs/.sw_v2.lic
                          : ./.configs/.swfeature.lic
Certificate file           : card:/atmf/lok/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands show atmf provision nodes

atmf provision node locate

Overview This command changes the present working directory to the directory of a provisioned node. This makes it easier to edit files and create a unique provisioned node in the backup.

This command can only be run on AMF master nodes.

Syntax

```
atmf provision node <nodename> locate
```

Parameter	Description
<nodename>	The name of the provisioned node.

Mode Privileged Exec

Usage This command is only available on master nodes in the AMF network. The command will only work if the provisioned node specified in the command has already been set up. Otherwise, an error message is shown when the command is run.

NOTE: *We advise that after running this command, you return to a known working directory, typically flash.*

Example To change the working directory that happens to be on device1 to the directory of provisioned node device2, use the following command:

```
device1# atmf provision node device2 locate
```

The directory of the node device2 should now be the working directory. You can use the command pwd to check this, as shown in the following figure.

Figure 40-6: Sample output from the **pwd** command

```
device2#pwd
card:/atmf/building_2/nodes/device2/flash
```

The output above shows that the working directory is now the flash of device2.

Related commands

atmf provision node create

atmf provision node clone

pwd

atmf reboot-rolling

Overview This command enables you to reboot the nodes in an AMF working-set, one at a time, as a rolling sequence in order to minimize downtime. Once a rebooted node has finished running its configuration and its ports are up, it re-joins the AMF network and the next node is rebooted.

By adding the *url* parameter, you can also upgrade your devices' software one AMF node at a time.

The **force** parameter forces the rolling reboot to continue even if a previous node does not rejoin the AMF network. Without the **force** parameter, the unsuitable node will time-out and the rolling reboot process will stop. However, with the **force** parameter applied, the process will ignore the timeout and move on to reboot the next node in the sequence.

This command can take a significant amount of time to complete.

Syntax `atmf reboot-rolling [force] [<url>]`

Parameter	Description
`force`	Ignore a failed node and move on to the next node. Where a node fails to reboot a timeout is applied based on the time taken during the last reboot.
`<url>`	The path to the software upgrade file.

Mode Privileged Exec

Usage You can load the software from a variety of locations. The latest compatible release for a node will be selected from your selected locatio, based on the parameters and URL you have entered.

For example card:/5.4.6/x*-5.4.6-*.rel will select from the folder card:/5.4.6 the latest file that matches the selection x (wildcard) -5.4.6-(wildcard).rel. Because x* is applied, each device type will be detected and its appropriate release file will be installed.

Other allowable entries are:

Entry	Used when loading software
card:*.rel:	from an SD card
tftp:<*ip-address*>:	from a TFTP server
usb:	from a USB flash drive
flash:	from flash memory, e.g. from one x610 switch to another
scp:	using secure copy
http:	from an HTTP file server

Several checks are performed to ensure the upgrade will succeed. These include checking the current node release boots from flash. If there is enough space on flash, the software release is copied to flash to a new location on each node as it is processed. The new release name will be updated using the **boot system**<*release-name*> command, and the old release will become the backup release file.

NOTE: *If you are using TFTP or HTTP, for example, to access a file on a remote device then the URL should specify the exact release filename without using wild card characters.*

On bootup the software release is verified. Should an upgrade fail, the upgrading unit will revert back to its previous software version. At the completion of this command, a report is run showing the release upgrade status of each node.

NOTE: *Take care when removing external media or rebooting your devices. Removing an external media while files are being written entails a significant risk of causing a file corruption.*

Example 1 To reboot all x510 nodes in an AMF network, use the following command:

```
Bld2_Floor_1# atmf working-set group x510
```

This command returns the following type of screen output:

```
====================
node1, node2, node3:
====================

Working set join

AMF_NETWORK[3]#
```

```
ATMF_NETWORK[3]# atmf reboot-rolling
```

When the reboot has completed, a number of status screens appear. The selection of these screens will depend on the parameters set.

```
Bld2_Floor_1#atmf working-set group x510

============================
SW_Team1, SW_Team2, SW_Team3:
============================

Working set join

ATMF_NETWORK[3]#atmf reboot-rolling
ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)
---------------------------
SW_Team1               14
SW_Team2                8
SW_Team3                8
Continue the rolling reboot ? (y/n):y
================================================
ATMF Rolling Reboot: Rebooting SW_Team1
================================================

% SW_Team1 has left the working-set
Reboot of SW_Team1 has completed
================================================
ATMF Rolling Reboot: Rebooting SW_Team2
================================================

% SW_Team2 has left the working-set
Reboot of SW_Team2 has completed
================================================
ATMF Rolling Reboot: Rebooting SW_Team3
================================================

% SW_Team3 has left the working-set
Reboot of SW_Team3 has completed

================================================
ATMF Rolling Reboot Complete
Node Name           Reboot Status
---------------------------------
SW_Team1               Rebooted
SW_Team2               Rebooted
SW_Team3               Rebooted
================================================
```

Example 2 To update firmware releases, use the following command:

```
Node_1# atmf working-set group all

ATMF_NETWORK[9]# atmf reboot-rolling
card:/5.4.6/x*-5.4.6-*.rel
```

```
ATMF Rolling Reboot Nodes:

                    Timeout
Node Name           (Minutes)    New Release File             Status
-------------------------------------------------------------------------
SW_Team1               8         x510-5.4.6-0.1.rel           Release Ready
SW_Team2              10         x510-5.4.6-0.1.rel           Release Ready
SW_Team3               8         ---                          Not Supported
HW_Team1               6         ---                          Incompatible
Bld1_Floor_2           2         x610-5.4.6-0.1.rel           Release Ready
Bld1_Floor_1           4         ---                          Incompatible
Building_1             2         ---                          Incompatible
Building_2             2         x908-5.4.6-0.1.rel           Release Ready
Continue upgrading releases ? (y/n):
```

atmf recover

Overview This command is used to manually initiate the recovery (or replication) of an AMF node, usually when a node is being replaced.

Syntax

```
atmf recover [<node-name> master <node-name>]
atmf recover [<node-name> controller <node-name>]
```

Parameter	Description
<node-name>	The name of the device whose configuration is to be recovered or replicated.
`master` *<node-name>*	The name of the master device that holds the required configuration information. Note that although you can omit both the node name and the master name; you cannot specify a master name unless you also specify the node name.
`controller` *<node-name>*	The name of the controller that holds the required configuration information. Note that although you can omit both the node name and the controller name; you cannot specify a controller name unless you also specify the node name.

Mode Privileged Exec

Usage The recovery/replication process involves loading the configuration file for a node that is either about to be replaced or has experienced some problem. You can specify the configuration file of the device being replaced by using the *<node-name>* parameter, and you can specify the name of the master node or controller holding the configuration file.

If the *<node-name>* parameter is not entered then the node will attempt to use one that has been previously configured. If the replacement node has no previous configuration (and has no previously used node-name), then the recovery will fail.

If the master or controller name is not specified then the device will poll all known AMF masters and controllers and execute an election process (based on the last successful backup and its timestamp) to determine which to use. If no valid backup master or controller is found, then this command will fail.

No error checking occurs when this command is run. Regardless of the last backup status, the recovering node will attempt to load its configuration from the specified master node or controller.

If the node has previously been configured, we recommend that you suspend any AMF backup before running this command. This is to prevent corruption of the backup files on the AMF master as it attempts to both backup and recover the node at the same time.

Example To recover the AMF node named Node_10 from the AMF master node named Master_2, use the following command:

```
Master_2# atmf recover Node_10 master Master_2
```

Related Commands

atmf backup stop

show atmf backup

show atmf

atmf recover guest

Overview Use this command to initiate a guest node recovery or replacement by reloading its backup file-set that is located within the AMF backup system. Note that this command must be run on the edge node device that connects to the guest node.

Syntax

```
atmf recover guest [<guest-port>]
```

Parameter	Description
<guest-port>	The port number that connects to the guest node.

Mode User Exec/Privileged Exec

Example To recover a guest on node1 port1.0.1, use the following command

```
node1# atmf recover guest port1.0.1
```

Related Commands show atmf backup guest

atmf recover led-off

Overview This command turns off the recovery failure flashing port LEDs. It reverts the LED's function to their normal operational mode, and in doing so assists with resolving the recovery problem. You can repeat this process until the recovery failure has been resolved. For more information, see the AMF Feature Overview and Configuration Guide.

Syntax
```
atmf recover led-off
```

Default Normal operational mode

Mode Privileged Exec

Example To revert the LEDs on Node1 from recovery mode display to their normal operational mode, use the command:

```
Node1# atmf recover led-off
```

Related Commands atmf recover

atmf remote-login

Overview Use this command to remotely login to other AMF nodes in order to run commands as if you were a local user of that node.

Syntax

```
atmf remote-login [user <name>] <nodename>
```

Parameter	Description
<name>	User name.
<nodename>	Node name.

Mode Privileged Exec (This command will only run at privilege level 15)

Usage You do not need a valid login on the local device in order to run this command. The session will take you to the enable prompt on the new device. If the remote login session exits for any reason (e.g. device reboot) you will be returned to the originating node.

The software will not allow you to run multiple remote login sessions. You must exit an existing session before starting a new one.

If you disconnect from the VTY session without first exiting from the AMF remote session, the device will keep the AMF remote session open until the exec-timeout time expires (10 minutes by default). If the exec-timeout time is set to infinity (**exec-timeout 0 0**), then the device is unable to ever close the remote session. To avoid this, we recommend you use the **exit** command to close AMF remote sessions, instead of closing the associated VTY sessions. We also recommend you avoid setting the exec-timeout to infinity.

Example 1 To remotely login from node Node10 to Node20, use the following command:

```
Node10# atmf remote-login node20
Node20>
```

Example 2 To close the session on Node20 and return to Node10's command line, use the following command:

```
Node20# exit
Node10#
```

Example 3 In this example, user Whitney is a valid user of node5. She can remotely login from node5 to node3 by using the following commands:

```
node5# atmf remote-login user whitney node3
node3> enable
```

NOTE: *In the above example the user name whitney is valid on both nodes.Therefore, to prevent unauthorized access, user names should be unique across all nodes within the AMF network.*

atmf restricted-login

Overview This command restricts the use of the atmf working-set on page 1603 command on all AMF master nodes to privilege 15 users only. Once entered on any AMF master node, this command will propagate across the network.

Note that once you have run this command, certain other commands that utilize the AMF working-set command, such as the **include**, **atmf reboot-rolling** and **show atmf group members** commands, will operate only on master nodes.

Use the **no** variant of this command to disable restricted login on the AMF network. This allows access to the **atmf working-set** command from any node in the AMF network.

Syntax

```
atmf restricted-login
no atmf restricted-login
```

Mode Privileged Exec

Default Master nodes operate with **atmf restricted-login** disabled.

Member nodes operate with **atmf restricted-login** enabled.

NOTE: *The default conditions of this command vary from those applied by its "no" variant. This is because the restricted-login action is only applied by **master** nodes, and in the absence of a master node, the default is to apply the restricted action to all **member** nodes with AMF configured.*

*In the presence of a **master** node, its default of "atmf restricted-login disabled" will permeate to all its member nodes. Similarly, any change in this command's status that is made on a master node, will also permeate to all its member nodes*

Example To enable restricted login, use the command

```
Node_20(config)# atmf restricted-login node20
```

Validation Command show atmf

atmf select-area

Overview Use this command to access devices in an area outside the core area on the controller network. This command will connect you to the remote area-master of the specified area.

This command is only valid on AMF controllers.

The **no** variant of this command disconnects you from the remote area-master.

Syntax

```
atmf select-area {<area-name>|local}
no atmf select-area
```

Parameter	Description
<area-name>	Connect to the remote area-master of the area with this name.
local	Return to managing the local controller area.

Mode Privileged Exec

Usage After running this command, use the atmf working-set command to select the set of nodes you want to access in the remote area.

Example To access nodes in the area Canterbury, use the command

```
controller-1# atmf select-area Canterbury
```

This displays the following output:

```
Test_network[3]#atmf select-area Canterbury
=============================================
Connected to area Canterbury via host Avensis:
=============================================
```

To return to the local area for controller-1, use the command

```
controller-1# atmf select-area local
```

Alternatively, to return to the local area for controller-1, use the command

```
controller-1# no atmf select-area
```

Related Commands atmf working-set

atmf virtual-link

Overview This command creates one or more Layer 2 tunnels that enable AMF nodes to transparently communicate across a wide area network using Layer 2 connectivity protocols.

Once connected through the tunnel, the remote member will have the same AMF capabilities as a directly connected AMF member.

Use the **no** variant of this command to remove the specified virtual link.

Syntax

```
atmf virtual-link id <1-4094> ip <a.b.c.d> remote-id <1-4094>
remote-ip <a.b.c.d> [remote-area <area-name>]
```

```
no atmf virtual-link id <1-4094>
```

Parameter	Description
`ip`	The Internet Protocol (IP).
<a.b.c.d>	The IP address, of the local amf node (at its interface to the tunnel) entered in a.b.c.d format.
`remote-id`	The ID of the (same) tunnel that will be applied by the remote node. Note that this must match the local-id that is defined on the remote node. This means that (for the same tunnel) the local and remote tunnel IDs are reversed on the local and remote nodes.
<1-4094>	The ID range 1-4094.
`remote-ip`	The IP address of the remote node
<a.b.c.d>	The IP address, of the remote node (at its interface to the tunnel) entered in a.b.c.d format.
`remote-area`	The remote area connected to this area virtual link
<area-name>	The name of the remote area connected to this virtual link.

Mode Global Configuration

Usage The Layer 2 tunnel that this command creates enables a local AMF session to appear to pass transparently across a Wide Area Network (WAN) such as the Internet. The addresses configured as the local and remote tunnel IP addresses must have IP connectivity to each other. If the tunnel is configured to connect a head office and branch office over the Internet, typically this would involve using some type of managed WAN service such as a site-to-site VPN. Tunnels are only supported using IPv4.

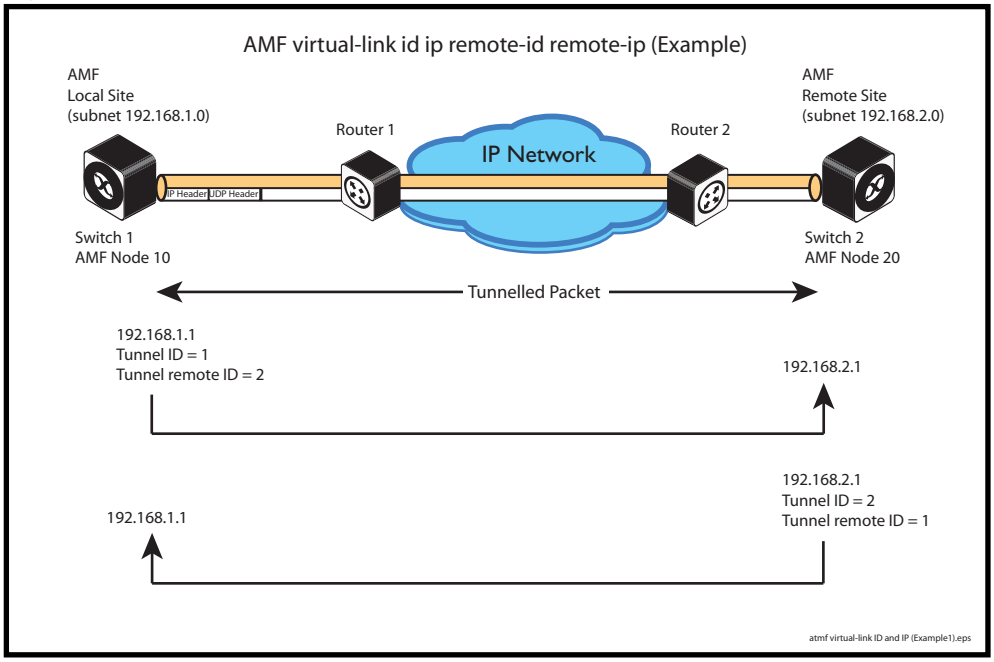
Configuration involves creating a local tunnel ID, a local IP address, a remote tunnel ID and a remote IP address. A reciprocal configuration is also required on the corresponding remote device. The local tunnel ID must be unique to the device on which it is configured.

The tunneled link may operate via external (non AlliedWare Plus) routers in order to provide wide area network connectivity. However in this configuration, the routers perform a conventional router to router connection. The protocol tunneling function is accomplished by the AMF nodes.

NOTE: *AMF cannot achieve zero touch replacement of the remote device that terminates the tunnel connection, because you must pre-configure the local IP address and tunnel ID on that remote device.*

Example 1 Use the following commands to create the tunnel shown in the figure below.

Figure 40-7: AMF virtual link example




```
Node_10(config)# atmf virtual-link id 1 ip 192.168.1.1
remote-id 2 remote-ip 192.168.2.1
```

```
Node_20(config)# atmf virtual-link id 2 ip 192.168.2.1
remote-id 1 remote-ip 192.168.1.1
```

Example 2 To set up an area virtual link to a remote site (assuming IP connectivity between the sites already), one site must run the following commands:

```
SiteA# configure terminal
```

```
SiteA(config)# atmf virtual-link id 5 ip 192.168.100.1
remote-id 10 remote-ip 192.168.200.1 remote-area SiteB-AREA
```

The second site must run the following commands:

```
SiteB# configure terminal
```

```
SiteB(config)# atmf virtual-link id 10 ip 192.168.200.1
remote-id 5 remote-ip 192.168.100.1 remote-area SiteA-AREA
```

Before you can apply the above **atmf virtual-link** command, you must configure the area names *SiteB-AREA* and *SiteA-AREA*.

Validation Command show atmf

show atmf links

atmf working-set

Overview Use this command to execute commands across an individually listed set of AMF nodes or across a named group of nodes.

Note that this command can only be run on a master node.

Use the **no** variant of this command to remove members or groups from the current working-set.

Syntax

```
atmf working-set {[<node-list>]|[group
{<group-list>|all|local|current}]}
```

```
no atmf working-set {[<node-list>]|[group <group-list>]}
```

Parameter	Description
<node-list>	A comma delimited list (without spaces) of nodes to be included in the working-set.
`group`	The AMF group.
<group-list>	A comma delimited list (without spaces) of groups to be included in the working-set. Note that this can include either defined groups, or any of the Automatic, or Implicit Groups shown earlier in the bulleted list of groups.
`all`	All nodes in the AMF.
`local`	Local node Running this command with the parameters **group local** will return you to the local prompt and local node connectivity.
`current`	Nodes in current list.

Mode Privileged Exec

Usage You can put AMF nodes into groups by using the atmf group (membership) command.

This command opens a session on multiple network devices. When you change the working set to anything other than the local device, the prompt will change to the AMF network name, followed by the size of the working set, shown in square brackets. This command has to be run at privilege level 15.

In addition to the user defined groups, the following system assigned groups are automatically created:

- Implicit Groups
  - local: The originating node.
  - current: All nodes that comprise the current working-set.
  - all: All nodes in the AMF.

- Automatic Groups - These can be defined by hardware architecture, e.g. x510, x610, x8100, AR3050S or AR4050S, or by certain AMF nodal designations such as master.

Note that the Implicit Groups do not appear in show atmf group command output.

If a node is an AMF master it will be automatically added to the master group.

Example 1 To add all nodes in the AMF to the working-set, use the command:

```
node1# atmf working-set group all
```

NOTE: *This command adds the implicit group "all" to the working set, where "all" comprises all nodes in the AMF.*

This command displays an output screen similar to the one shown below:

```
=========================================
node1, node2, node3, node4, node5, node6:
=========================================

Working set join

ATMF_NETWORK_Name[6]#
```

Example 2 To return to the local prompt, and connect to only the local node, use the command:

```
ATMF_Network_Name[6]# atmf working-set group local
node1#
```

The following table describes the meaning of the prompts in this example.

Parameter	Description
ATMF_Network_Name	The name of the AMF network, as set by the atmf network-name command.
[6]	The number of nodes in the working-set.
node1	The name of the local node, as set by the hostname command.

clear atmf links statistics

Overview This command resets the values of all AMF link, port, and global statistics to zero.

Syntax
```
clear atmf links statistics
```

Mode Privilege Exec

Example To reset the AMF link statistics values, use the command:

```
node_1# clear atmf links statistics
```

Related Commands show atmf links statistics

debug atmf

Overview This command enables the AMF debugging facilities, and displays information that is relevant (only) to the current node. The detail of the debugging displayed depends on the parameters specified.

If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

The **no** variant of this command disables either all AMF debugging information, or only the particular information as selected by the command's parameters.

Syntax

```
debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```

```
no debug atmf
[link|crosslink|arealink|database|neighbor|error|all]
```

Parameter	Description
`link`	Output displays debugging information relating to uplink or downlink information.
`crosslink`	Output displays all crosslink events.
`arealink`	Output displays all arealink events.
`database`	Output displays only notable database events.
`neighbor`	Output displays only notable AMF neighbor events.
`error`	Output displays AMF error events.
`all`	Output displays all AMF events.

Default All debugging facilities are disabled.

Mode User Exec and Global Configuration

Usage If no additional parameters are specified, then the command output will display all AMF debugging information, including link events, topology discovery messages and all notable AMF events.

NOTE: *An alias to the **no** variant of this command is undebug atmf on page 1689.*

Examples To enable all AMF debugging, use the command:

```
node_1# debug atmf
```

To enable AMF uplink and downlink debugging, use the command:

```
node_1# debug atmf link
```

To enable AMF error debugging, use the command:

```
node_1# debug atmf error
```

Related Commands no debug all

debug atmf packet

Overview This command configures AMF Packet debugging parameters. The debug only displays information relevant to the current node. The command has following parameters:

Syntax

```
debug atmf packet[[direction {rx|tx|both}][level
{1|2|3}][timeout <seconds>][num-pkts <quantity>][filter node
<name> [interface <ifname>][pkt-type
{[1][2][3][4][5][6][7][8][9][10][11][12][13]]]
```

Simplified Syntax

`debug atmf packet`	`[direction {rx|tx|both}]`
	`[level {[1][2|3}]`
	`[timeout <seconds>]`
	`[num-pkts <quantity>]`
`debug atmf packet filter`	`[node <name>]`
	`[interface <ifname>]`
	`[pkt-type [1][2][3][4][5][6][7][8][9][10][11][12][13]]`

NOTE: *You can combine the syntax components shown, but when doing so, you must retain their original order.*

Default Level 1, both Tx and Rx, a timeout of 60 seconds with no filters applied.

NOTE: *An alias to the **no** variant of this command - undebug atmf - can be found elsewhere in this chapter.*

Mode User Exec and Global Configuration

Usage If no additional parameters are specified, then the command output will apply a default selection of parameters shown below:

Parameter	Description
`direction`	Sets debug to packet received, transmitted, or both
`rx`	packets received by this node
`tx`	Packets sent from this node
`1`	AMF Packet Control header Information, Packet Sequence Number. Enter 1 to select this level.
`2`	AMF Detailed Packet Information. Enter 2 to select this level.
`3`	AMF Packet HEX dump. Enter 3 to select this level.

Parameter	Description
`timeout`	Sets the execution timeout for packet logging
<seconds>	Seconds
`num-pkts`	Sets the number of packets to be dumped
<quantity>	The actual number of packets
`filter`	Sets debug to filter packets
`node`	Sets the filter on packets for a particular Node
<name>	The name of the remote node
`interface`	Sets the filter to dump packets from an interface (portx.x.x) on the local node
<ifname>	Interface port or virtual-link
`pkt-type`	Sets the filter on packets with a particular AMF packet type
`1`	Crosslink Hello BPDU packet with crosslink links information. Enter 1 to select this packet type.
`2`	Crosslink Hello BPDU packet with downlink domain information. Enter 2 to select this packet type.
`3`	Crosslink Hello BPDU packet with uplink information. Enter 3 to select this packet type.
`4`	Downlink and uplink hello BPDU packets. Enter 4 to select this packet type.
`5`	Non broadcast hello unicast packets. Enter 5 to select this packet type.
`6`	Stack hello unicast packets. Enter 6 to select this packet type.
`7`	Database description. Enter 7 to select this packet type.
`8`	DBE request. Enter 8 to select this packet type.
`9`	DBE update. Enter 9 to select this packet type.
`10`	DBE bitmap update. Enter 10 to select this packet type.
`11`	DBE acknowledgment. Enter 11 to select this packet type.
`12`	Area Hello Packets. Enter 12 to select this packet type.
`13`	Gateway Hello Packets. Enter 13 to select this packet type.

Examples To set a packet debug on node 1 with level 1 and no timeout, use the command:

```
node_1# debug atmf packet direction tx timeout 0
```

To set a packet debug with level 3 and filter packets received from AMF node 1:

```
node_1# debug atmf packet direction tx level 3 filter node_1
```

To enable send and receive 500 packets only on vlink1 for packet types 1, 7, and 11, use the command:

```
node_1# debug atmf packet num-pkts 500 filter interface vlink1
pkt-type 1 7 11
```

This example applies the **debug atmf packet** command and combines many of its options:

```
node_1# debug atmf packet direction rx level 1 num-pkts 60
filter node x610 interface port1.0.1 pkt-type 4 7 10
```

discovery

Overview AMF nodes gather information about guest nodes by using one of two internally defined discovery methods: static or dynamic. This is one of several modal commands that are configured from within its specific guest-class (mode).

Dynamic discovery (the default method) involves learning IP address and MAC addresses of guest nodes from protocols outside of AMF such as LLDP or DHCP snooping. Dynamic learning is only supported when using IPv4. For IPv6 the static discovery method must be used.

Note that if the discovery method is dynamic, you should ensure that the command ip dhcp snooping delete-by-linkdown is set.

The static method involves entering the guest class name and IP address using the switchport atmf-guestlink command to separately assign an individual switch port to each of the guest nodes. The MAC addresses of each of the guests of that class can then be learned from ARP or Neighbor discovery tables. If you are using the static discovery method, you must ensure that you have configured the appropriate class type for each of your statically discovered guest nodes.

The **no** variant of this command returns the discovery method to **dynamic**.

Syntax

```
discovery [static|dynamic]
no discovery
```

Parameter	Description
`static`	Statically assigned
`dynamic`	Learned from DCHCPSN or LLDP

Default Dynamic

Mode ATMF Guest Configuration Mode

Usage This command is one of several modal commands that are configured and applied for a specific guest-class (mode) and whose settings are automatically applied to a guest-node link by the switchport atmf-guestlink command.

Example 1 To configure the discovery of the guest-class camera to operate statically, use the following commands:

```
Node1#conf t
Node1(config)#atmf guest-class camera
Node1(config-guest)#discovery static
Node1(config-guest)#end
```

Example 2 To return the discovery method for the guest class TQ4600-1 to its default of **dynamic**, use the following commands:

```
Node1#conf t
Node1(config)#atmf guest-class TQ4600-1
Node1(config-guest)#no discovery
Node1(config-guest)#end
```

Related Commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf nodes

erase factory-default

Overview This command erases all data from NVS and all data from flash **excluding** the following:

- The current release file and its /flash/.release file
- The backup release file and /flash/.backup file
- v1 license files /flash/.configs/.swfeature.lic
- v2 license files /flash/.configs/.sw_v2.lic

The device is then rebooted and returns the device to its factory default condition. The device can then be used for automatic node recovery.

Syntax

```
erase factory-default
```

Mode Global Configuration.

Usage This command is an alias to the atmf cleanup command.

Example To erase data, use the command:

```
Node_1(config)# erase factory-default
This command will erase all NVS, all flash contents except for
the boot release, and any license files, and then reboot the
switch. Continue? (y/n):y
```

Related Commands atmf cleanup

http-enable

Overview This command is used to enable GUI access to a guest node. When http-enable is configured the port number is set to its default of 80. If the guest node is using a different port for HTTP, you can configure this using the port *<PORTNO>* attribute.

This command is used to inform the GUI that this device has an HTTP interface at the specified port number so that a suitable URL can be provided to the user.

Use the **no** variant of this command to disable HTTP.

Syntax

```
http-enable [port <PORTNO>]
no http-enable
```

Parameter	Description
`port`	TCP port number.
<PORTNO>	The port number to be configured.

Default http-enable is off.
If http-enable is selected without a port parameter the port number will default to 80.

Mode ATMF Guest Configuration Mode

Example 1 To enable HTTP access on port 80 (the default) of a guest node, use the following commands:

```
node1# conf t
node1(config)#atmf guest-class Camera
node1(config-atmf-guest)#http-enable
node1(config-atmf-guest)#
```

Example 2 To enable HTTP access on port 400 of a guest node, use the following commands:

```
node1# conf t
node1(config)#atmf guest-class Camera
node1(config-atmf-guest)#http-enable port 400
node1(config-atmf-guest)#
```

Example 3 To disable HTTP access of a guest node, use the following commands:

```
node1# conf t
node1(config)#atmf guest-class Camera
node1(config-atmf-guest)#no http-enable
node1(config-atmf-guest)#
```

Related Commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf nodes

modeltype

Overview This command sets the expected model type of the guest node. Guest nodes can be one of various types: alliedware, aw+, tq or other. The model type will default to **other** if nothing is set.

Use the **no** variant of this command to reset the model type to **other**.

Syntax

```
modeltype [alliedware|aw+|tq|other]
```

Parameter	Description
`alliedware`	A legacy Allied Telesis operating system.
`aw+`	The Allied Telesis AlliedWare Plus operating system.
`tq`	An Allied Telesis TQ Series wireless access point.
`other`	Used where the model type is outside the above definitions.

Default Will default to **other**

Mode ATMF Guest Configuration Mode

Example 1 To assign the model type **tq** to the guest-class called **tq_device**, use the following commands:

```
node1# conf t
node1(config)# atmf guest-class tq_device
node1(config-atmf-guest)# modeltype tq
node1(config-atmf-guest)# end
```

Example 2 To remove the model type **tq** from the guest-class called **tq_device,** and reset it to the default of **other**, use the following commands:

```
node1# conf t
node1(config)# atmf guest-class tq_device
node1(config-atmf-guest)# no modeltype
node1(config-atmf-guest)# end
```

Related Commands

atmf guest-class

switchport atmf-guestlink

show atmf links guest

show atmf

Overview Displays information about the current AMF node.

Syntax

```
show atmf [summary|tech|nodes|session]
```

Parameter	Description
`summary`	Displays summary information about the current AMF node.
`tech`	Displays global AMF information.
`nodes`	Displays a list of AMF nodes together with brief details.
`session`	Displays information on an AMF session.

Default Only summary information is displayed.

Mode User Exec and Privileged Exec

Usage AMF uses internal VLANs to communicate between nodes about the state of the AMF network. Two VLANs have been selected specifically for this purpose. Once these have been assigned, they are reserved for AMF and cannot be used for other purposes

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Example 1 To show summary information on AMF node_1 use the following command:

```
node_1# show atmf summary
```

Table 1: Output from the **show atmf summary** command

```
node_1#show atmf summary
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : Test_network
Node Name              : node_1
Role                   : Master
Restricted login       : Disabled
Current ATMF Nodes     : 3
```

Example 2 To show information specific to AMF nodes use the following command:

```
node_1# show atmf nodes
```

Example 3 The **show amf session** command displays all CLI (Command Line Interface) sessions for users that are currently logged in and running a CLI session.

To display AMF active sessions, use the following command:

```
node_1# show atmf session
```

For example, in the output below, node_1 and node_5 have active users logged in.

Table 2: Output from the **show atmf session** command

```
node_1#show atmf session

CLI Session Neighbors

Session ID                          : 73518
Node Name                           : node_1
PID                                 : 7982
Link type                           : Broadcast-cli
MAC Address                         : 0000.0000.0000
Options                             : 0
Our bits                            : 0
Link State                          : Full
Domain Controller                   : 0
Backup Domain Controller            : 0
Database Description Sequence Number : 00000000
First Adjacency                     : 1
Number Events                       : 0
DBE Retransmit Queue Length         : 0
DBE Request List Length             : 0
Session ID                          : 410804
Node Name                           : node_5
PID                                 : 17588
Link type                           : Broadcast-cli
MAC Address                         : 001a.eb56.9020
Options                             : 0
Our bits                            : 0
Link State                          : Full
Domain Controller                   : 0
Backup Domain Controller            : 0
Database Description Sequence Number : 00000000
First Adjacency                     : 1
Number Events                       : 0
DBE Retransmit Queue Length         : 0
DBE Request List Length             : 0
```

Example 4 The AMF tech command collects all the AMF commands, and displays them. You can use this command when you want to see an overview of the AMF network.

To display AMF technical information, use the following command:

```
node_1# show atmf tech
```

Table 3: Output from the **show atmf tech** command

```
node_1#show atmf tech
ATMF Summary Information:

ATMF Status           : Enabled
Network Name          : ATMF_NET
Node Name             : node_1
Role                  : Master
Current ATMF Nodes    : 8

ATMF Technical information:

Network Name                        : ATMF_NET
Domain                              : node_1's domain
Node Depth                          : 0
Domain Flags                        : 0
Authentication Type                 : 0
MAC Address                         : 0014.2299.137d
Board ID                            : 287
Domain State                        : DomainController
Domain Controller                   : node_1
Backup Domain Controller            : node2
Domain controller MAC               : 0014.2299.137d
Parent Domain                       : -
Parent Domain Controller            : -
Parent Domain Controller MAC        : 0000.0000.0000
Number of Domain Events             : 0
Crosslink Ports Blocking            : 0
Uplink Ports Waiting on Sync        : 0
Crosslink Sequence Number           : 7
Domains Sequence Number             : 28
Uplink Sequence Number              : 2
Number of Crosslink Ports           : 1
Number of Domain Nodes              : 2
Number of Neighbors                 : 5
Number of Non Broadcast Neighbors   : 3
Number of Link State Entries        : 1
Number of Up Uplinks                : 0
Number of Up Uplinks on This Node   : 0
DBE Checksum                        : 84fc6
Number of DBE Entries               : 0
Management Domain Ifindex           : 4391
Management Domain VLAN              : 4091
Management ifindex                  : 4392
Management VLAN                     : 4092
```

Table 4: Parameter definitions from the **show atmf tech** command

Parameter	Definition
ATMF Status	The Node's AMF status, either Enabled or Disabled.
Network Name	The AMF network that a particular node belongs to.

Table 4: Parameter definitions from the **show atmf tech** command (cont.)

Parameter	Definition
Node Name	The name assigned to a particular node.
Role	The role configured for this AMF device, either Master or Member.
Current ATMF Nodes	The count of AMF nodes in an AMF Network.
Node Address	An address used to access a remotely located node (.atmf).
Node ID	A unique identifier assigned to a Node on an AMF network.
Node Depth	The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
Domain State	The state of Node in a Domain in AMF network as Controller/Backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between Nodes of different domain (up/down links). • VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. • Management Subnet - Network prefix for the subnet. • Management IP Address - The IP address allocated for this traffic. • Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).
Domain VLAN	The VLAN assigned for traffic between Nodes of same domain (crosslink). • VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. • Domain Subnet. The subnet address used for this traffic. • Domain IP Address. The IP address allocated for this traffic. • Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).
Device Type	The Product Series name.
ATMF Master	Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).
SC	The device configuration, one of C - Chassis (SBx8100 Series), S - Stackable (VCS) or N - Standalone.
Parent	The node to which the current node has an active uplink.
Node Depth	The number of nodes in the path from this node to the master node.

Related Commands show atmf detail

show atmf area

Overview Use this command to display information about an AMF area. On AMF controllers, this command displays all areas that the controller is aware of. On remote AMF masters, this command displays the controller area and the remote local area. On gateways, this command displays the controller area and remote master area.

Syntax `show atmf area [detail] [<area-name>]`

Parameter	Description
`detail`	Displays detailed information
`<area-name>`	Displays information about master and gateway nodes in the specified area only.

Mode Privileged Exec

Example 1 To show information about all areas, use the command:

```
controller-1# show atmf area
```

The following figure shows example output from running this command on a controller.

Table 5: Example output from the **show atmf area** command on a Controller.

```
controller-1#show atmf area

  ATMF Area Information:

  * = Local area

  Area               Area   Local         Remote        Remote         Node
  Name               ID     Gateway       Gateway       Master         Count
-------------------------------------------------------------------------
* NZ                 1      Reachable     N/A           N/A             3
  Wellington         2      Reachable     Reachable     Auth OK         120
  Canterbury         3      Reachable     Reachable     Auth Error      -
  SiteA-AREA         14     Unreachable   Unreachable   Unreachable     -
  Auckland           100    Reachable     Reachable     Auth Start      -
  Southland          120    Reachable     Reachable     Auth OK         54

  Area count:        6                            Area node count:     177
```

The following figure shows example output from running this command on a remote master.

Table 6: Example output from the **show atmf area** command on a remote master.

```
Canterbury#show atmf area

  ATMF Area Information:

  * = Local area

  Area               Area   Local          Remote         Remote          Node
  Name               ID     Gateway        Gateway        Master          Count
-------------------------------------------------------------------------------
  NZ                 1      Reachable      N/A            N/A              -
* Canterbury         3      Reachable      N/A            N/A              40

  Area count:        2                        Local area node count:      40
```

Table 7: Parameter definitions from the **show atmf area** command

Parameter	Definition
*	Indicates the area of the device on which the command is being run.
Area Name	The name of each area.
Area ID	The ID of the area.
Local Gateway	Whether the local gateway node is reachable or not.
Remote Gateway	Whether the remote gateway node is reachable or not. This is one of the following: • Reachable, if the link has been established. • Unreachable, if a link to the remote area has not been established. This could mean that a port or vlan is down, or that inconsistent VLANs have been configured using the switchport atmf-arealink remote-area command. • N/A for the area of the controller or remote master on which the command is being run, because the gateway node on that device is local. • Auth Start, which may indicate that the area names match on the controller and remote master, but the IDs do not match. • Auth Error, which indicates that the areas tried to authenticate but there is a problem. For example, the passwords configured on the controller and remote master may not match, or a password may be missing on the remote master.? • Auth OK, which indicates that area authentication was successful and you can now use the atmf select-area command.
Remote Master	Whether the remote master node is reachable or not. This is N/A for the area of the controller or remote master on which the command is being run, because the master node on that device is local.
Node Count	The number of nodes in the area.
Area Count	The number of areas controlled by the controller.
Area Node Count	The total number of nodes in the area.

Example 2 To show detailed information about the areas, use the command:

```
controller-1# show atmf area detail
```

The following figure shows example output from running this command.

Table 8: Output from the **show atmf area detail** command

```
controller-1#show atmf area detail

 ATMF Area Detail Information:

 Controller distance       : 0

 Controller Id             : 21
 Backup Available          : FALSE

 Area Id                   : 2
 Gateway Node Name         : controller-1
 Gateway Node Id           : 342
 Gateway Ifindex           : 6013
 Masters Count             : 1
 Master Node Name          : well-master (329)
 Node Count                : 2

 Area Id                   : 3
 Gateway Node Name         : controller-1
 Gateway Node Id           : 342
 Gateway Ifindex           : 4511
 Masters Count             : 2
 Master Node Name          : cant1-master (15)
 Master Node Name          : cant2-master (454)
 Node Count                : 2
```

Related Commands

show atmf area summary

show atmf area nodes

show atmf area nodes-detail

show atmf area guests

Overview This command will display details of all guests that the controller is aware of.

Syntax

```
show atmf area guests [<area-name> [<node-name>]]
```

Parameter	Description
<area-name>	The area name for guest information
<node-name>	The name of the node that connects to the guests.

Default N/A

Mode User Exec/Privileged Exec

Example 1 To display atmf area guest nodes on a controller, use the command,

```
GuestNode[1]#show atmf area guests
```

Output Figure 40-8: Example output from the **show atmf area guests** command

```
main-building Area Guest Node Information:
Device          MAC                                          IP/IPv6
Type            Address         Parent          Port         Address
-------------------------------------------------------------------------------
-               0008.5d10.7635  x230            1.0.3        192.168.5.4
AT-TQ4600       eccd.6df2.da60  wireless-node1  1.0.4        192.168.5.3
-               0800.239e.f1fe  x230            1.0.4        192.168.4.8
AT-TQ4600       001a.eb3b.dc80  wireless-node2  1.0.7        192.168.4.12

main-building guest node count 4

GuestNode[1]#
```

Table 9: Parameters in the output from **show atmf area guests** command

Parameter	Description
Device Type	The device type as read from the guest node.
MAC Address	The MAC address of the guest-node
Parent	The device that directly connects to the guest-node
Port	The port number on the parent node that connects to the guest node.
IP/IPv6	The IP or IPv6 address of the guest node.

Related Commands

show atmf area

show atmf area nodes

show atmf backup guest

show atmf area guests-detail

show atmf area guests-detail

Overview This command displays the local and remote guest information from an AMF controller.

Syntax

```
show atmf area guests-detail [<area-name> [<node-name>]]
```

Parameter	Description
<area-name>	The name assigned to the AMF area. An area is an AMF network that is under the control of an AMF Controller.
<node-name>	The name assigned to the network node.

Default N/A.

Mode Privileged Exec

Example To display detailed information for all guest nodes attached to "node1", which is located within the area named "northern", use the following command:

```
AMF_controller#show atmf area guests-detail northern node1
```

Output Figure 40-9: Example output from the **show atmf guest detail** command.

```
#show atmf guest detail

Node Name                       : Node1
Port Name                       : port1.0.5
Ifindex                         : 5005
Guest Description               : tq4600
Device Type                     : AT-TQ4600
Configuration Mismatch          : No
Backup Supported                : Yes
MAC Address                     : eccd.6df2.da60
IP Address                      : 192.168.4.50
IPv6 Address                    : Not Set
HTTP Port                       : 80
Firmware Version                :
Node Name                       : poe
Port Name                       : port1.0.6
Ifindex                         : 5006
Guest Description               : tq3600
Device Type                     : AT-TQ2450
Configuration Mismatch          : No
Backup Supported                : Yes
MAC Address                     : 001a.eb3b.cb80
IP Address                      : 192.168.4.9
IPv6 Address                    : Not Set
HTTP Port                       : 80
Firmware Version                :
```

Table 10: Parameters shown in the output of the **show atmf guest detail** command

Parameter	Description
`Node Name`	The name of the guest's parent node.
`Port Name`	The port on the parent node that connects to the guest.
`IFindex`	An internal index number that maps to the port number on the parent node.
`Guest Description`	A brief description of the guest node as manually entered into the description (interface) command for the guest node port on the parent node.
`Device Type`	The device type as supplied by the guest node itself.
`Backup Supported`	Indicates whether AMF supports backup of this guest node.
`MAC Address`	The MAC address of the guest node.
`IP Address`	The IP address of the guest node.
`IPv6 Address`	The IPv6 address of the guest node.
`HTTP Port`	The HTTP port enables you to specify a port when enabling http to allow a URL for the http user interface of a Guest Node. This is determined by the http-enable command.
`Firmware Version`	The firmware version that the guest node is currently running.

Related Commands

show atmf area nodes-detail

show atmf area guests

show atmf area nodes

Overview Use this command to display summarized information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

Syntax

```
show atmf area nodes [<area-name> [<node-name>]]
```

Parameter	Description
<area-name>	Displays information about nodes in the specified area.
<node-name>	Displays information about the specified node.

Mode Privileged Exec

Usage If you do not limit the output to a single area or node, this command lists all remote nodes that the controller is aware of. This can be a very large number of nodes.

Example To show summarized information about all the nodes the controller is aware of, use the command:

```
controller-1# show atmf area nodes
```

The following figure shows partial example output from running this command.

Table 11: Output from the **show atmf area nodes** command

```
controller-1#show atmf area nodes

 Wellington Area Node Information:

 Node         Device             ATMF                                Node
 Name         Type               Master  SC    Parent                Depth
 ---------------------------------------------------------------------------
 well-gate    x210-24GT          N       N     well-master             1
 well-master  AT-x930-28GPX      Y       N     none                    0

Wellington node count 2

...
```

Table 12: Parameter definitions from the **show atmf area nodes** command

Parameter	Definition
Node Name	The name assigned to a particular node.
Device Type	The Product series name.

Table 12: Parameter definitions from the **show atmf area nodes** command (cont.)

Parameter	Definition
ATMF Master	Whether the node is an AMF master node for its area ('Y' if it is and 'N' if it is not).
SC	The device configuration, one of C - Chassis (SBx8100 series), S - Stackable (VCS) or N - Standalone.
Parent	The node to which the current node has an active uplink.
Node Depth	The number of nodes in the path from this node to the master node.

Related Commands

show atmf area

show atmf area nodes-detail

show atmf area nodes-detail

Overview Use this command to display detailed information about an AMF controller's remote nodes.

Note that this command can only be run from a controller node.

Syntax

```
show atmf area nodes-detail [<area-name> [<node-name>]]
```

Parameter	Description
<area-name>	Displays detailed information about nodes in the specified area.
<node-name>	Displays detailed information about the specified node.

Mode Privileged Exec

Usage If you do not limit the output to a single area or node, this command displays information about all remote nodes that the controller is aware of. This can be a very large number of nodes.

Example To show information about all the nodes the controller is aware of, use the command:

```
controller-1# show atmf area nodes-detail
```

The following figure shows partial example output from running this command.

Table 13: Output from the **show atmf area nodes-detail** command

```
controller-1#show atmf area nodes-detail

Wellington Area Node Information:
  Node name  well-gate
  Parent node name    : well-master
  Domain id           : well-gate's domain
  Board type          : 368
  Distance to core    : 1
  Flags               : 50
  Extra flags         : 0x00000006
  MAC Address         : 001a.eb56.9020

Node name well-master
  Parent node name    : none
  Domain id           : well-master's domain
  Board type          : 333
  Distance to core    : 0
  Flags               : 51
  Extra flags         : 0x0000000c
  MAC Address         : eccd.6d3f.fef7

...
```

Table 14: Parameter definitions from the **show atmf area nodes-detail** command

Parameter	Definition
Node name	The name assigned to a particular node.
Parent node name	The node to which the current node has an active uplink.
Domain id	
Board type	The Allied Telesis code number for the device.
Distance to core	The number of nodes in the path from the current node to the master node in its area.
Flags	Internal AMF information
Extra flags	Internal AMF information
MAC Address	The MAC address of the current node

Related Commands

show atmf area

show atmf area nodes

show atmf area summary

Overview Use this command to display a summary of IPv6 addresses used by AMF, for one or all of the areas controlled by an AMF controller.

Syntax

```
show atmf area summary [<area-name>]
```

Parameter	Description
<area-name>	Displays information for the specified area only.

Mode Privileged Exec

Example 1 To show a summary of IPv6 addresses used by AMF, for all of the areas controlled by controller-1, use the command:

```
controller-1# show atmf area summary
```

The following figure shows example output from running this command.

Table 15: Output from the **show atmf area summary** command

```
controller-1#show atmf area summary

 ATMF Area Summary Information:

Management Information
 Local IPv6 Address              : fd00:4154:4d46:1::15

Area Information
 Area Name                       : NZ (Local)
 Area ID                         : 1
 Area Master IPv6 Address        : -

 Area Name                       : Wellington
 Area ID                         : 2
 Area Master IPv6 Address        : fd00:4154:4d46:2::149

 Area Name                       : Canterbury
 Area ID                         : 3
 Area Master IPv6 Address        : fd00:4154:4d46:3::f

 Area Name                       : Auckland
 Area ID                         : 100
 Area Master IPv6 Address        : fd00:4154:4d46:64::17
 Interface                       : vlink2000
```

Related Commands

show atmf area

show atmf area nodes

show atmf area nodes-detail

show atmf backup

Overview This command displays information about AMF backup status for all the nodes in an AMF network. It can only be run on AMF master and controller nodes.

Syntax

```
show atmf backup [logs|server-status|synchronize [logs]]
```

Parameter	Description
`logs`	Displays detailed log information.
`server-status`	Displays connectivity diagnostics information for each configured remote file server.
`synchronize`	Display the file server synchronization status
`logs`	For each remote file server, display the logs for the last synchronization

Mode Privileged Exec

Example 1 To display the AMF backup information, use the command:

```
node_1# show atmf backup
```

To display log messages to do with backups, use the command:

```
node_1# show atmf backup logs
```

Table 40-1: Output from **show atmf backup**

```
Node_1# show atmf backup
ScheduledBackup ......Enabled
  Schedule.............1 per day starting at 03:00
  Next Backup Time....19 May 2015 03:00
Backup Bandwidth .....Unlimited
Backup Media..........SD (Total 1974.0 MB, Free197.6MB)
Current Action........Starting manual backup
Started...............18 May 2012 10:08
CurrentNode...........atmf_testbox1
Backup Redundancy ..... Enabled
  Local media ......... SD (Total 3788.0MB, Free 3679.5MB)
  State ............... Active

Node Name                Date         Time      In ATMF  On Media   Status
-------------------------------------------------------------------------------
atmf_testbox1            17 May 2014  09:58:59  Yes      Yes        Good
atmf_testbox2            17 May 2014  10:01:23  Yes      Yes        Good
```

Table 40-2: Output from **show atmf backup logs**

```
Node_1#show atmf backup logs

Backup Redundancy ..... Enabled
Local media ......... SD (Total 3788.0MB, Free 1792.8MB)
State ............... Inactive (Remote file server is not available)

Log File Location: card:/atmf/ATMF/logs/rsync_<node name>.log

Node
Name Log Details
-------------------------------------------------------------------------------
atmf_testbox
2015/08/25 18:16:51 [9045] receiving file list
2015/08/25 18:16:51 [9047] .d..t.... flash/
2015/08/25 18:16:52 [9047] >f+++++++ flash/a.rel
```

Example 2 To display the AMF backup synchronization status, use the command:

```
node_1# show atmf backup synchronize
```

To display log messages to do with synchronization of backups, use the command:

```
node_1# show atmf backup synchronize logs
```

Table 40-3: Output from **show atmf backup synchronize**

```
Node_1#show atmf backup synchronize

ATMF backup synchronization:

 * = Active file server

  Id  Date          Time       Status
-------------------------------------------------------------------
-
  1   14 Aug 2014   22:25:57   Synchronized
* 2   -             -          Active
```

Table 40-4: Output from **show atmf backup synchronize logs**

```
Node_1#show atmf backup synchronize logs

Id    Log Details
-------------------------------------------------------------------------------
1     2014/08/14 22:25:54 [8039] receiving file list
      2014/08/14 22:25:54 [8039] >f..t.... backup_Box1.info
      2014/08/14 22:25:54 [8039] sent 46 bytes received 39 bytes total size 40
```

Example 3 To display the AMF backup information with the optional parameter **server-status**, use the command:

```
Node_1# show atmf backup server-status
```

```
Node1#sh atmf backup server-status

Id   Last Check    State
-------------------------------------
1    186 s         File server ready
2    1 s           SSH no route to host
```

Table 41: Parameter definitions from the **show atmf backup** command

Parameter	Definition
Scheduled Backup	Indicates whether AMF backup scheduling is enabled or disabled.
Schedule	Displays the configured backup schedule.
Next Backup Time	Displays the date and time of the next scheduled.
Backup Media	The current backup medium in use. This will be one of USB, SD, or NONE. Utilized and available memory (MB) will be indicated if backup media memory is present.
Current Action	The task that the AMF backup mechanism is currently performing. This will be a combination of either (Idle, Starting, Doing, Stopping), or (manual, scheduled).
Started	The date and time that the currently executing task was initiated in the format DD MMM YYYY HH:MM
Current Node	The name of the node that is currently being backed up.
Backup Redundancy	Whether backup redundancy is enabled or disabled.
Local media	The local media to be used for backup redundancy; SD or USB or NONE, and total and free memory available on the media.
State	Whether SD or USB media is installed and available for backup redundancy. May be Active (if backup redundancy is functional—requires both the local redundant backup media and a remote server to be configured and available) or Inactive.
Node Name	The name of the node that is storing backup data - on its backup media.
Date	The data of the last backup in the format DD MMM YYYY.
Time	The time of the last backup in the format HH:MM:SS.
In ATMF	Whether the node shown is active in the AMF network, (Yes or No).
On Media	Whether the node shown has a backup on the backup media (Yes or No).

Table 41: Parameter definitions from the **show atmf backup** command (cont.)

Parameter	Definition
`Status`	The output can contain one of four values: • "-" meaning that the status file cannot be found or cannot be read. • "Errors" meaning that there are issues - note that the backup may still be deemed successful depending on the errors. • "Stopped" meaning that the backup attempt was manually aborted;. • "Good" meaning that the backup was completed successfully.
`Log File Location`	All backup attempts will generate a result log file in the identified directory based on the node name. In the above example this would be: card:/amf/office/logs/rsync_amf_testbox1.log.
`Log Details`	The contents of the backup log file.
`server-status`	Displays connectivity diagnostics information for each configured remove file server.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related Commands

show atmf

atmf network-name

show atmf backup area

Overview Use this command to display backup status information for the master nodes in one or more areas.

Note that this command is only available on AMF controllers.

Syntax `show atmf backup area [<area-name> [<node-name>]] [logs]`

Parameter	Description
`logs`	Displays the logs for the last backup of each node.
`<area-name>`	Displays information about nodes in the specified area.
`<node-name>`	Displays information about the specified node.

Mode Privileged Exec

Example To show information about backups for an area, use the command:

```
controller-1# show atmf backup area
```

Table 42: Output from the **show atmf backup area** command

```
controller-1#show atmf backup area

Scheduled Backup ...... Enabled
  Schedule ............ 12 per day starting at 14:30
  Next Backup Time .... 15 Apr 2015 04:30
Backup Bandwidth ...... Unlimited
Backup Media .......... FILE SERVER 1 (Total 128886.5MB, Free 26234.2MB)
Server Config .........
 * 1 .................. Configured   (Mounted, Active)
    Host ............... 10.37.74.1
    Username ........... root
    Path ............... /tftpboot/backups_from_controller-1
    Port ............... -
   2 .................. Configured   (Unmounted)
    Host ............... 10.37.142.1
    Username ........... root
    Path ............... -
    Port ............... -
Current Action ........ Idle
  Started ............. -
  Current Node ........ -

Backup Redundancy ..... Enabled
  Local media ......... USB (Total 7604.0MB, Free 7544.0MB)
  State ............... Active

Area Name          Node Name            Id   Date          Time       Status
-------------------------------------------------------------------------------
Wellington         camry                1    15 Apr 2015   02:30:22   Good
Canterbury         corona               1    15 Apr 2015   02:30:23   Good
Canterbury         Avensis              1    15 Apr 2015   02:30:22   Good
Auckland           RAV4                 1    15 Apr 2015   02:30:23   Good
Southland          MR2                  1    15 Apr 2015   02:30:24   Good
```

Related Commands

atmf backup area-masters enable

show atmf area

show atmf area nodes-detail

switchport atmf-arealink remote-area

show atmf backup guest

Overview This command displays backup status information of guest nodes in an AMF network.This command can only be run on a device configured as an AMF Master and has an AMF guest license.

Syntax

```
show atmf backup guest [<node-name> [<guest-port>]] [logs]
```

Parameter	Description
<node-name>	The name of parent guest node
<guest-port>	The port number on the parent node

Mode User Exec/Privileged Exec

Example On the switch named x930-master, to display information about the AMF backup guest status, use the command:

```
x930-master# show atmf backup guest
```

Output Figure 40-10: Example output from **show atmf backup guest**

```
x930-master#sh atmf backup guest
Guest Backup .......... Enabled
Scheduled Backup ...... Disabled
  Schedule ............ 1 per day starting at 03:00
  Next Backup Time .... 20 Jan 2016 03:00
Backup Bandwidth ...... Unlimited
Backup Media .......... FILE SERVER 2 (Total 655027.5MB,
                        Free 140191.5MB)
Server Config
 1 ................... Configured (Mounted)
 Host ............... 11.0.24.1
 Username ........... bob
 Path ............... guest-project
 Port ............... -
* 2 ................... Configured (Mounted, Active)
 Host ............... 11.0.24.1
 Username ........... bob
 Path ............... guest-project-second
Port..................-
Current Action .......Idle
Started ............. -
Current Node ........ -
Backup Redundancy ....Enabled
Local media ......... USB (Total 7376.0MB, Free 7264.1MB)
State ............... Active
```

```
Parent Node Name      Port Name        Id     Date           Time          Status
-------------------------------------------------------------------------------
x230                  port1.0.4        2      19 Jan 2016    22:21:46      Good
                                       1      19 Jan 2016    22:21:46      Good
                                       USB    19 Jan 2016    22:21:46      Good
```

Table 40-1: Parameters in the output from **show atmf backup guest**

Parameter	Description
Guest Backup	The status of the guest node backup process
Scheduled Backup	The timing configured for guest backups.
Schedule	Displays the configured backup schedule.
Next Backup Time	The time the next backup process will be initiated.
Backup Bandwidth	The bandwidth limit applied to the backup data flow measured in kilo Bytes /second. Note that unlimited means there is no limit set specifically for the backup data flow.
Backup Media	Detail of the memory media used to store the backup files and the current memory capacity available.

Related Commands

show atmf backup area

show atmf backup

show atmf links guest

show atmf nodes

show atmf backup guest

atmf backup guests delete

atmf backup guests enable

show atmf detail

Overview This command displays details about an AMF node. It can only be run on AMF master and controller nodes.

Syntax

```
show atmf detail
```

Parameter	Description
`detail`	Displays output in greater depth.

Mode Privileged Exec

Example 1 To display the AMF node1 information in detail, use the command:

```
controller-1# show atmf detail
```

A typical output screen from this command is shown below:

```
atmf-1#show atmf detail
ATMF Detail Information:

Network Name                        : Test_network
Network Mtu                         : 1300
Node Name                           : controller-1
Node Address                        : controller-1.atmf
Node ID                             : 342
Node Depth                          : 0
Domain State                        : BackupDomainController
Recovery State                      : None
Log Verbose Setting                 : Verbose

Management VLAN
 VLAN ID                            : 4000
 Management Subnet                  : 172.31.0.0
 Management IP Address              : 172.31.1.86
 Management Mask                    : 255.255.128.0
 Management IPv6 Address            : fd00:4154:4d46:1::156
 Management IPv6 Prefix Length      : 64

Domain VLAN
 VLAN ID                            : 4091
 Domain Subnet                      : 172.31.128.0
 Domain IP Address                  : 172.31.129.86
 Domain Mask                        : 255.255.128.0
```

Table 41: Parameter definitions from the **show atmf detail** command

Parameter	Definition
`Network MTU`	The network MTU for the ATMF network.
`Network Name`	The AMF network that a particular node belongs to.
`Node Name`	The name assigned to a particular node.
`Node Address`	An Address used to access a remotely located node. This is simply the Node Name plus the dotted suffix atmf (.atmf).
`Node ID`	A Unique identifier assigned to a Node on an AMF network.
`Node Depth`	The number of nodes in path from this node to level of the AMF root node. It can be thought of as the vertical depth of the AMF network from a particular node to the zero level of the AMF root node.
`Domain State`	The state of Node in a Domain in AMF network as Controller/Backup.
`Recovery State`	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - Auto, Manual, or None.
`Management VLAN`	The VLAN created for traffic between Nodes of different domain (up/down links). • VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. • Management Subnet - Network prefix for the subnet. • Management IP Address - The IP address allocated for this traffic. • Management Mask - The subnet mask used to create a subnet for this traffic (255.255.128.0).
`Domain VLAN`	The VLAN assigned for traffic between Nodes of same domain (crosslink). • VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. • Domain Subnet. The subnet address used for this traffic. • Domain IP Address. The IP address allocated for this traffic. • Domain Mask. The subnet mask used to create a subnet for this traffic (255.255.128.0).
`Node Depth`	The number of nodes in the path from this node to the Core domain.

show atmf group

Overview This command can be used to display the group membership within to a particular AMF node. It can also be used with the working-set command to display group membership within a working set.

Each node in the AMF is automatically added to the group that is appropriate to its hardware architecture, e.g. x510, x610. Nodes that are configured as masters are automatically assigned to the master group.

You can create arbitrary groups of AMF members based on your own selection criteria. You can then assign commands collectively to any of these groups.

Syntax
```
show atmf group [user-defined|automatic]
```

Parameter	Description
`user-defined`	User-defined-group information display.
`automatic`	Automatic group information display.

Default All groups are displayed

Mode Privileged Exec

Example 1 To display group membership of node2, use the following command:

```
node2# show atmf group
```

A typical output screen from this command is shown below:

```
ATMF group information

master, x510

node2#
```

This screen shows that node2 contains the groups **master** and **x510**. Note that although the node also contains the implicit groups, these do not appear in the show output.

Example 2 The following commands (entered on *node2*) will display all the automatic groups within the working set containing *node1* and all nodes that have been pre-defined to contain the *sysadmin* group:

First define the working-set:

```
node1# #atmf working-set node1 group sysadmin
```

A typical output screen from this command is shown below:

```
ATMF group information

master, poe, x8100


================================================
node1, node2, node3, node4, node5, node6:
================================================

ATMF group information

sysadmin, x8100

AMF_NETWORK[6]#
```

This confirms that the six nodes (*node1* to *node6*) are now members of the working-set and that these nodes reside within the *AMF-NETWORK*.

Note that to run this command, you must have previously entered the command atmf working-set on page 1603. This can be seen from the network level prompt, which in this case is *AMF_NETWORK[6]#*.

Table 42: Sample output from the **show atmf group** command for a working set.

```
AMF_NETWORK[6]#show atmf group
==============================
node3, node4, node5, node6:
==============================

ATMF group information

edge_switches, x510
```

Table 43: Parameter definitions from the **show atmf group** command for a working set

Parameter	Definition
`ATMF group information`	Displays a list of nodes and the groups that they belong to, for example: • master - Shows a common group name for Nodes configured as AMF masters. • Hardware Arch - Shows a group for all Nodes sharing a common Hardware architecture, e.g. x8100, x610, for example. • User-defined - Arbitrary groups created by the user for AMF nodes.

show atmf group members

Overview This command will display all group memberships within an AMF working-set. Each node in the AMF working set is automatically added to automatic groups which are defined by hardware architecture, e.g. x510, x610. Nodes that are configured as masters are automatically assigned to the master group. Users can define arbitrary groupings of AMF members based on their own criteria, which can be used to select groups of nodes.

Syntax

```
show atmf group members [user-defined|automatic]
```

Parameter	Description
`user-defined`	User defined group membership display.
`automatic`	Automatic group membership display.

Mode Privileged Exec

Example To display group membership of all nodes in a working-set, use the command:

```
ATMF_NETWORK[9]# show atmf group members
```

Table 44: Sample output from the **show atmf group members** command

```
ATMF Group membership

Automatic         Total
Groups            Members   Members
-----------------------------------------------------------
master            1         Building_1
poe               1         HW_Team1
x510              3         SW_Team1 SW_Team2 SW_Team3
x610              1         HW_Team1
x8100             2         Building_1 Building_2

ATMF Group membership

User-defined      Total
Groups            Members   Members
-----------------------------------------------------------
marketing           1       Bld1_Floor_1
software            3       SW_Team1 SW_Team2 SW_Team3
```

Table 45: Parameter definitions from the **show atmf group members** command

Parameter	Definition
`Automatic Groups`	Lists the Automatic Groups and their nodal composition. The sample output shows AMF nodes based on the same Hardware type or belonging to the same Master group.
`User-defined Groups`	Shows the grouping of AMF nodes in user defined groups.
`Total Members`	Shows the total number of members in each group.
`Members`	Shows the list of AMF nodes in each group.

Related Commands

show atmf group

show atmf

atmf group (membership)

show atmf guest

Overview This command is available on any AMF master in the network. It displays details about the AMF guest nodes that exist in the AMF network, such as device type, IP address and MAC address etc.

Syntax `show atmf guest [<node-name>] [<guest-port>]`

Parameter	Description
<node-name>	The name of the guest node's parent.
<guest-port>	The port name on the parent node.

Mode User Exec/Privileged Exec

Example To display the ATMF guest output, use the command:

```
awplus# show atmf guest
```

Output Figure 40-11: Example output from the **show atmf guest** command.

```
master#show atmf guests

  Guest Information:

  Device          Device          Parent      Guest     IP/IPv6
  Name            Type            Node        Port      Address
-------------------------------------------------------------------
  master-2.1.1    AR415S          master      2.1.1     192.168.2.10
  master-2.1.2    AT-9924T        master      2.1.2     192.168.1.10
  master-2.1.4    AT-TQ3200       master      2.1.4     192.168.1.12

  Current ATMF guest node count 3
```

Table 46: Parameters shown in the output of the **show atmf guest** command

Parameter	Description
Device Name	The name that is discovered from the device, or failing that, a name that is auto-assigned by AMF. The auto-assigned name consists of <parent node name>-<attached port number>
Device Type	This is the product name of the Guest Node and is discovered from the device. If no device Type can be discovered, then the modelName configured on the Guest-class assigned to the connected port is used.
Parent Node	The AMF member name of the AMF member that directly connects to the guest node.

Table 46: Parameters shown in the output of the **show atmf guest** command

Parameter	Description
`Guest Port`	The port, on the Parent node that directly connects to the guest node.
`IP/IPv6 Address`	The address discovered from the node, or statically configured on the parent node's attached port.

Related Commands

atmf guest-class

switchport atmf-guestlink

show atmf backup guest

show atmf links

Overview This command displays information about AMF links on a switch. The display output contains link status state information.

Syntax

```
show atmf links brief
```

Parameter	Description
`links`	AMF links.
`brief`	A brief summary of AMF links, their configuration and status.
`detail`	A detailed description of the AMF links.
`statistics`	AMF statistics.
`ifrange`	Limits the display output to the specified interface range.

Mode User Exec and Privileged Exec

Example 1 To display a brief summary of the AMF links, use the following command:

```
node-1# show atmf links brief
```

The following example summarizes the links that are detailed in the example in show atmf links.

Figure 40-12: Sample output from the **show atmf links brief** command

```
Example-core# show atmf links

ATMF Link Brief Information:

Local      Link       Link    ATMF         Adjacent       Adjacent    Link
Port       Type       Status  State        Node           Ifindex     State
-------------------------------------------------------------------------
1.0.10     Crosslink  Down    Init         *crosslink1     -          Blocking
1.0.14     Crosslink  Down    Init         *crosslink2     -          Blocking
1.0.1      Downlink   Down    Init         -               -          Blocking
1.0.2      Downlink   Up      Full         Node2           5001       Forwarding
1.0.8      Downlink   Up      Full         downlink1       5001       Forwarding

* = Provisioned.
```

Table 47: Parameter definitions from the **show atmf links brief** command output

Parameter	Definition
`Local Port`	Shows the local port on the selected node.
`Link Type`	Shows link type as Uplink or Downlink (parent and child) or Cross-link (nodes in same domain).
`Link Status`	Shows the link status of the local port on the node as either Up or Down.
`ATMF State`	Shows AMF state of the local port: • Init - Link is down. • Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable. • Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations. • OneWay - Link is up and has waited the hold down period and now attempting to link to • another unit in another domain • Full - Link hello packets are sent and received from its neighbor with its own node id. • Shutdown - Link has been shut down by user configuration.
`Adjacent Node`	Shows the Adjacent AMF Node to the one being configured.
`Adjacent IF Index`	Shows the IF index for the Adjacent AMF Node connected to the node being configured.
`Link State`	Shows the state of the AMF link. Valid states are either Forwarding or Blocking.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Mode User Exec and Privileged Exec

Related Commands

no debug all

clear atmf links statistics

show atmf

show atmf nodes

show atmf links detail

Overview This command displays detailed information on all the links configured in the AMF network. It can only be run on AMF master and controller nodes.

Syntax

```
show atmf links detail
```

Parameter	Description
`detail`	Detailed AMF links information.

Mode User Exec

Example To display the AMF link details use this command:

```
device1# show atmf links detail
```

The output from this command will display all the internal data held for AMF links. The following example gives details of the links that are summarized in the example in show atmf links.

Table 48: Sample output from the **show atmf links detail** command

```
device1# show atmf links detail

-------------------------------------------------------------------------------
Crosslink Ports Information
-------------------------------------------------------------------------------
Port                              : sa1
Ifindex                           : 4501
Port Status                       : Down
Port State                        : Init
Last event                        :
Port BPDU Receive Count           : 0
Port                              : po10
Ifindex                           : 4610
Port Status                       : Up
Port State                        : Full
Last event                        : AdjNodeLSEPresent
Port BPDU Receive Count           : 140
Adjacent Node Name                : Building-B
Adjacent Ifindex                  : 4610
Adjacent MAC                      : eccd.6dd1.64d0
Port Last Message Response        : 0
```

Table 48: Sample output from the **show atmf links detail** command (cont.)

```
Port                                : po30
Ifindex                             : 4630
Port Status                         : Up
Port State                          : Full
Last event                          : AdjNodeLSEPresent
Port BPDU Receive Count             : 132
Adjacent Node Name                  : Building-A
Adjacent Ifindex                    : 4630
Adjacent MAC                        : eccd.6daa.c861
Port Last Message Response          : 0

Link State Entries:

Crosslink Ports Blocking            : False
Node.Ifindex                        : Building-A.4630 - Example-core.4630
Transaction ID                      : 2 - 2
MAC Address                         : eccd.6daa.c861 - 0000.cd37.054b
Link State                          : Full - Full

Node.Ifindex                        : Building-B.4610 - Example-core.4610
Transaction ID                      : 2 - 2
MAC Address                         : eccd.6dd1.64d0 - 0000.cd37.054b
Link State                          : Full - Full

Domain Nodes Tree:

Node                                : Building-A
  Links on Node                     : 1
  Link 0                            : Building-A.4630 - Example-core.4630
  Forwarding State                  : Forwarding
Node                                : Building-B
  Links on Node                     : 1
  Link 0                            : Building-B.4610 - Example-core.4610
  Forwarding State                  : Forwarding
Node                                : Example-core
  Links on Node                     : 2
  Link 0                            : Building-A.4630 - Example-core.4630
  Forwarding State                  : Forwarding
  Link 1                            : Building-B.4610 - Example-core.4610
  Forwarding State                  : Forwarding
Crosslink Transaction Entries:

Node                                : Building-B
Transaction ID                      : 2
Uplink Transaction ID               : 6
Node                                : Building-A
Transaction ID                      : 2
Uplink Transaction ID               : 6

Uplink Information:

Waiting for Sync                    : 0
Transaction ID                      : 6
Number of Links                     : 0
Number of Local Uplinks             : 0
```

Table 48: Sample output from the **show atmf links detail** command (cont.)

```
Originating Node                    : Building-A
Domain                              : -'s domain
Node                                : Building-A
Ifindex                             : 0
Node Depth                          : 0
Transaction ID                      : 6
Flags                               : 32
Domain Controller                   : -
Domain Controller MAC               : 0000.0000.0000

Originating Node                    : Building-B
Domain                              : -'s domain
Node                                : Building-B
Ifindex                             : 0
Node Depth                          : 0
Transaction ID                      : 6
Flags                               : 32
Domain Controller                   : -
Domain Controller MAC               : 0000.0000.0000

Downlink Domain Information:

Domain                              : Dept-A's domain
  Domain Controller                 : Dept-A
  Domain Controller MAC             : eccd.6d20.c1d9
  Number of Links                   : 2
  Number of Links Up                : 2
  Number of Links on This Node      : 2
  Links are Blocked                 : 0
  Node Transaction List
    Node                            : Building-B
    Transaction ID                  : 8
    Node                            : Building-A
    Transaction ID                  : 8
  Domain List
    Domain                          : Dept-A's domain
      Node                          : Example-core
      Ifindex                       : 4621
      Transaction ID                : 8
      Flags                         : 1
    Domain                          : Dept-A's domain
      Node                          : Example-core
      Ifindex                       : 4622
      Transaction ID                : 8
      Flags                         : 1
```

Table 48: Sample output from the **show atmf links detail** command (cont.)

```
Domain                              : Dorm-D's domain
  Domain Controller                 : Dorm-D
  Domain Controller MAC             : 0000.cd37.082c
  Number of Links                   : 2
  Number of Links Up                : 2
  Number of Links on This Node      : 2
  Links are Blocked                 : 0
  Node Transaction List
    Node                            : Building-B
    Transaction ID                  : 20
    Node                            : Building-A
    Transaction ID                  : 20
  Domain List
    Domain                          : Dorm-D's domain
      Node                          : Building-A
      Ifindex                       : 0
      Transaction ID                : 20
      Flags                         : 32
    Domain                          : Dorm-D's domain
      Node                          : Building-B
      Ifindex                       : 0
      Transaction ID                : 20
      Flags                         : 32
    Domain                          : Dorm-D's domain
      Node                          : Example-core
      Ifindex                       : 4510
      Transaction ID                : 20
      Flags                         : 1
    Domain                          : Dorm-D's domain
      Node                          : Example-core
      Ifindex                       : 4520
      Transaction ID                : 20
      Flags                         : 1

Domain                              : Example-edge's domain
  Domain Controller                 : Example-edge
  Domain Controller MAC             : 001a.eb93.7aa6
  Number of Links                   : 1
  Number of Links Up                : 1
  Number of Links on This Node      : 0
  Links are Blocked                 : 0
  Node Transaction List
    Node                            : Building-B
    Transaction ID                  : 9
    Node                            : Building-A
    Transaction ID                  : 9
```

Table 48: Sample output from the **show atmf links detail** command (cont.)

```
  Domain List
    Domain                          : Example-edge's domain
      Node                          : Building-A
      Ifindex                       : 0
      Transaction ID                : 9
      Flags                         : 32
    Domain                          : Example-edge's domain
      Node                          : Building-B
      Ifindex                       : 5027
      Transaction ID                : 9
      Flags                         : 1
----------------------------------------------------------------
Up/Downlink Ports Information
----------------------------------------------------------------
Port                                : sa10
Ifindex                             : 4510
Port Status                         : Up
Port State                          : Full
Last event                          : LinkComplete
Adjacent Node                       : Dorm-A
Adjacent Internal ID                : 211
Adjacent Ifindex                    : 4510
Adjacent Board ID                   : 387
Adjacent MAC                        : eccd.6ddf.6cdf
Adjacent Domain Controller          : Dorm-D
Adjacent Domain Controller MAC      : 0000.cd37.082c
Port Forwarding State               : Forwarding
Port BPDU Receive Count             : 95
Port Sequence Number                : 11
Port Adjacent Sequence Number       : 7
Port Last Message Response          : 0
Port                                : po21
Ifindex                             : 4621
Port Status                         : Up
Port State                          : Full
Last event                          : LinkComplete
Adjacent Node                       : Dept-A
Adjacent Internal ID                : 29
Adjacent Ifindex                    : 4621
Adjacent Board ID                   : 340
Adjacent MAC                        : eccd.6d20.c1d9
Adjacent Domain Controller          : Dept-A
Adjacent Domain Controller MAC      : eccd.6d20.c1d9
Port Forwarding State               : Forwarding
Port BPDU Receive Count             : 96
Port Sequence Number                : 8
Port Adjacent Sequence Number       : 9
Port Last Message Response          : 0
Special Link Present                : FALSE
```

Table 49: Parameter definitions from the **show atmf links detail** command output

Parameter	Definition
`Crosslink Ports Information`	Show details of all Crosslink ports on this Node: • Port - Name of the Port or static aggregation (sa<*>). • Ifindex - Interface index for the crosslink port. • VR ID - Virtual router id for the crosslink port. • Port Status - Status of the local port on the Node as UP or DOWN. • Port State - AMF State of the local port. – Init - Link is down. – Hold - Link transitioned to up state, but waiting for hold period to ensure link is stable. – Incompatible - Neighbor rejected the link because of inconsistency in AMF configurations. – OneWay - Link is up and has waited the hold down period and now attempting to link to – another unit in another domain – Full - Link hello packets are sent and received from its neighbor with its own node id. – Shutdown - Link has been shut down by user configuration. Port BPDU Receive Count - The number of AMF protocol PDU's received. • Adjacent Node Name - The name of the adjacent node connected to this node. • Adjacent Ifindex - Adjacent AMF Node connected to this Node. • Adjacent VR ID - Virtual router id of the adjacent node in the domain. • Adjacent MAC - MAC address of the adjacent node in the domain. • Port Last Message Response - Response from the remote neighbor to our AMF last hello packet.
`Link State Entries`	Shows all the link state database entries: • Node.Ifindex - Shows adjacent Node names and Interface index. • Transaction ID - Shows transaction id of the current crosslink transaction. • MAC Address - Shows adjacent Node MAC addresses. • Link State - Shows AMF states of adjacent nodes on the link.
`Domain Nodes Tree`	Shows all the nodes in the domain: • Node - Name of the node in the domain. • Links on Node - Number of crosslinks on a vertex/node. • Link no - Shows adjacent Node names and Interface index. • Forwarding State - Shows state of AMF link Forwarding/Blocking.
`Crosslink Transaction Entries`	Shows all the transaction entries: • Node - Name of the AMF node. • Transaction ID - transaction id of the node. • Uplink Transaction ID - transaction id of the remote node.

Table 49: Parameter definitions from the **show atmf links detail** command output (cont.)

Parameter	Definition
`Uplink Information`	Show all uplink entries. • Waiting for Sync - Flag if uplinks are currently waiting for synchronization. • Transaction ID - Shows transaction id of the local node. • Number of Links - Number of up downlinks in the domain. • Number of Local Uplinks - Number of uplinks on this node to the parent domain. • Originating Node - Node originating the uplink information. • Domain - Name of the parent uplink domain. • Node - Name of the node in the parent domain, that is connected to the current domain. • Ifindex - Interface index of the parent node's link to the current domain. • VR ID - Virtual router id of the parent node's link to the current domain. • Transaction ID - Transaction identifier for the neighbor in crosslink. • Flags - Used in domain messages to exchange the state: ATMF_DOMAIN_FLAG_DOWN = 0 ATMF_DOMAIN_FLAG_UP = 1 ATMF_DOMAIN_FLAG_BLOCK = 2 ATMF_DOMAIN_FLAG_NOT_PRESENT = 4 ATMF_DOMAIN_FLAG_NO_NODE = 8 ATMF_DOMAIN_FLAG_NOT_ACTIVE_PARENT = 16 ATMF_DOMAIN_FLAG_NOT_LINKS = 32 ATMF_DOMAIN_FLAG_NO_CONFIG = 64 • Domain Controller - Domain Controller in the uplink domain • Domain Controller MAC - MAC address of Domain Controller in uplink domain
`Downlink Domain Information`	Shows all the downlink entries: • Domain - Name of the downlink domain. • Domain Controller - Controller of the downlink domain. • Domain Controller MAC - MAC address of the domain controller. • Number of Links - Total number of links to this domain from the Node. • Number of Links Up - Total number of links that are in UP state. • Number of Links on This Node - Number of links terminating on this node. • Links are Blocked - 0 links are not blocked to the domain. 1 All links are blocked to the domain.

Table 49: Parameter definitions from the **show atmf links detail** command output (cont.)

Parameter	Definition
`Node Transaction List`	List of transactions from this downlink domain node. • Node - 0 links are not blocked to the domain. 1 All links are blocked to the domain. • Transaction ID - Transaction id for this node. • Domain List: Shows list of nodes in the current domain and their links to the downlink domain.: • Domain - Domain name of the downlink node. • Node - Name of the node in the current domain. • Ifindex - Interface index for the link from the node to the downlink domain. • Transaction ID - Transaction id of the node in the current domain. • Flags - As mentioned above.
`Up/Downlink Ports Information`	Shows all the configured up and down link ports on this node: • Port - Name of the local port. • Ifindex - Interface index of the local port. • VR ID - Virtual router id for the local port. • Port Status - Shows status of the local port on the Node as UP/DOWN. • Port State - AMF state of the local port. • Adjacent Node - nodename of the adjacent node. • Adjacent Internal ID - Unique node identifier of the remote node. • Adjacent Ifindex - Interface index for the port of adjacent AMF node. • Adjacent Board ID - Product identifier for the adjacent node. • Adjacent VR ID - Virtual router id for the port on adjacent AMF node. • Adjacent MAC - MAC address for the port on adjacent AMF node. • Adjacent Domain Controller - nodename of the Domain controller for Adjacent AMF node. • Adjacent Domain Controller MAC - MAC address of the Domain controller for Adjacent AMF node. • Port Forwarding State - Local port forwarding state Forwarding or Blocking. • Port BPDU Receive Count - count of AMF protocol PDU's received. • Port Sequence Number - hello sequence number, incremented every time the data in the hello packet changes. • Port Adjacent Sequence Number - remote ends sequence number used to check if we need to process this packet or just note it arrived. • Port Last Message Response - response from the remote neighbor to our last hello packet.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related Commands

no debug all

clear atmf links statistics

show atmf

show atmf links guest

Overview This command displays information about guest nodes visible to an AMF device.

Syntax

```
show atmf links guest [detail] [interface <IFRANGE>]
```

Parameter	Description
`detail`	Displays a full output for the connected guest nodes
<IFRANGE>	Select a specific range of ports to display.

Default With no parameters specified this command will display its standard output for all ports with guest nodes connected.

Mode User Exec/Privileged Exec

Example 1 To display information about AMF guests that are connectable from node1, use the command:

```
node1# show atmf links guest
```

Output Figure 40-13: Example of standard output from **show atmf links guest**

```
node1#sh atmf links guest

Guest Link Information:

DC = Discovery configuration
  S = static D = dynamic

Local    Guest         Model        MAC             IP / IPv6
Port     Class         Type      DC Address         Address
-----------------------------------------------------------------
1.0.1    -             other     D  0013.1a1e.4589  192.168.1.2
1.0.2    aastra-phone  other     D  0008.5d10.7635  192.168.1.3
1.0.3    cisco-phone2  other     S  -               192.168.2.1
1.0.4    panasonic...  other     D  0800.239e.f1fe  192.168.1.5
```

Example 2 To display detailed information about AMF guests, use the command:

```
node1# show atmf links guest detail
```

Output Figure 40-14: Example of output from **show atmf links guest detail**

```
Detailed Guest Link Information:

Interface           : port1.0.1
  Class Name        : -
  Model Type        : other
  Discovery Method  : Dynamic
  IP Address        : 192.168.1.2
  State             : Getting ID
  MAC address       : 0013.1a1e.4589

Interface           : port1.0.2
  Class Name        : aastra-phone
  Model Type        : other
  Discovery Method  : Dynamic
  IP Address        : 192.168.1.3
  State             : Full
  MAC address       : 0008.5d10.7635
  Device Type       : Aastra IP Phone

Interface           : port1.0.4
  Class Name        : panasonic-camera
  Model Type        : other
  Discovery Method  : Dynamic
  IP Address        : 192.168.1.5
  State             : Getting ID
  MAC address       : 0800.239e.f1fe
```

Table 40-1: Parameters shown in the output of **show atmf links guest**

Parameter	Description
Interface	The port on the parent node that connects to the guest.
Class Name	The name of the ATMF guest-class that has been assigned to the guest node by the atmf guest-class command.
Model-Type	The model type of the guest node, as entered by the modeltype command. Can be one of the following: • alliedware • aw+ • tq • other
Discovery Method	The discovery method as applied by the discovery command. This can be either dynamic or static.
IP Address	The IP address of the guest node.
State	
MAC Address	The MAC address of the guest node.

Related Commands

atmf guest-class

discovery

http-enable

username

modeltype

switchport atmf-guestlink

show atmf backup guest

show atmf links statistics

Overview This command displays details of the AMF links configured on the device and also displays statistics about the AMF packet exchanges between the devices.

It is also possible to display the AMF link configuration and packet exchange statistics for a specified interface.

This command can only be run on AMF master and controller nodes

Syntax `show atmf links statistics [interface [<port_number>]]`

Parameter	Description
`interface`	Specifies that the command applies to a specific interface (port) or range of ports. Where both the interface and port number are unspecified, full statistics (not just those relating to ports will be displayed.
<port_number>	Enter the port number for which statistics are required. A port range, a static channel or LACP link can also be specified. Where no port number is specified, statistics will be displayed for all ports on the device.

Mode User Exec

Example 1 To display AMF link statistics for the whole device, use the command:

```
device1# show atmf links statistics
```

Table 41: Sample output from the **show atmf links statistics** command

```
ATMF Statistics:

                                  Receive        Transmit
------------------------------------------------------------------------------
Arealink Hello                      318            327
Crosslink Hello                     164            167
Crosslink Hello Domain              89             92
Crosslink Hello Uplink              86             88
Hello Link                          0              0
Hello Neighbor                      628            630
Hello Stack                         0              0
Hello Gateway                       1257           1257
Database Description                28             28
Database Request                    8              6
Database Update                     66             162
Database Update Bitmap              0              29
Database Acknowledge                144            51
```

Table 41: Sample output from the **show atmf links statistics** command (cont.)

```
Transmit Fails                      0             1
Discards                            0             0
Total ATMF Packets                  2788          2837

ATMF Database Statistics:

Database Entries                    18
Database Full Ages                  0
ATMF Virtual Link Statistics:

Virtual                             Receive                   Transmit
link                  Receive       Dropped      Transmit     Dropped
-------------------------------------------------------------------------------
vlink2000             393           0            417          0

ATMF Packet Discards:
Type0   0           : Gateway hello msg received from unexpected neighbor
Type1   0           : Stack hello msg received from unexpected neighbor
Type2   0           : Discard TX update bitmap packet - bad checksum
Type3   0           : Discard TX update packet - neighbor not in correct state
Type4   0           : Discard update packet - bad checksum or type
Type5   0           : Discard update packet - neighbor not in correct state
Type6   0           : Discard update bitmap packet - bad checksum or type
Type7   0           : Incarnation is not possible with the data received
Type8   0           : Discard crosslink hello received - not correct state
Type9   0           : Discard crosslink domain hello received on non crosslink
Type10  0           : Discard crosslink domain hello - not in correct state
Type11  0           : Crosslink uplink hello received on non crosslink port
Type12  0           : Discard crosslink uplink hello - not in correct state
Type13  0           : Wrong network-name for this ATMF
Type14  0           : Packet received on port is too long
Type15  0           : Bad protocol version, received on port
Type16  0           : Bad packet checksum calculation
Type17  0           : Bad authentication type
Type18  0           : Bad simple password
Type19  0           : Unsupported authentication type
Type20  0           : Discard packet - unknown neighbor
Type21  0           : Discard packet - port is shutdown
Type22  0           : Non broadcast hello msg received from unexpected neighbor
Type23  0           : Arealink hello msg received on non arealink port
Type24  0           : Discard arealink hello packet - not in correct state
Type25  0           : Discard arealink hello packet - failed basic processing
Type26  0           : Discard unicast packet - MAC address does not match node
Type27  0           : AMF Master license node limit exceeded
```

Example 2 To display the AMF links statistics on interface port1.0.5, use the command:

```
device1# show atmf links statistics interface
port1.0.5
```

Figure 40-15: Sample output from the **show atmf links statistics** command for interface 1.0.5

```
device1# show atmf links statistics interface port1.0.5

ATMF Port Statistics:

Transmit                                    Receive

port1.0.5  Crosslink Hello                  231             232
port1.0.5  Crosslink Hello Domain           116             116
port1.0.5  Crosslink Hello Uplink           116             115
port1.0.5  Hello Link                       0               0
port1.0.5  Arealink Hello                   0               0
```

Figure 40-16: Parameter definitions from the **show atmf links statistics** command output

Parameter	Definition
Receive	Shows a count of AMF protocol packets received per message type.
Transmit	Shows the number of AMF protocol packets transmitted per message type.
Database Entries	Shows the number of AMF elements existing in the distributed database.
Database Full Ages	Shows the number of times the entries aged in the database.
ATMF Packet Discards	Shows the number of discarded packets of each type.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related Commands

no debug all

clear atmf links statistics

show atmf

show atmf memory (deprecated)

Overview This command has been deprecated in Software Version 5.4.5-0.1 and later. To see details of AMF memory usage, please use the following commands instead:

- show memory allocations atmfd
- show memory pools atmfd

show atmf nodes

Overview This command displays nodes currently configured within the AMF network and presents a topographical representation of the network infrastructure.

This command displays a summary of all virtual links currently in the running configuration.

Syntax

```
show atmf nodes [guest|all]
```

Parameter	Description
guest	Display only guest nodes in the AMF network.
all	Display all nodes in the AMF network

Mode Privileged Exec

Example 1 To display AMF information for guest nodes only, use the command:

```
node_1# show atmf nodes guest
```

Table 42: Sample output from the **show atmf nodes guest** command

```
node1#show atmf nodes guest

Guest Information:
Device        MAC                                    IP/IPv6
Name          Address         Parent           Port  Address
-------------------------------------------------------------------------------
aastra-...    0008.5d10.7635  Node-1           1.0.2 192.168.4.7
poe-1.0.1     0013.1a1e.4589  Node-1           1.0.1 192.168.4.6
ip-camera     0800.239e.f1fe  Node-1           1.0.4 192.168.4.8
tq4600        eccd.6df2.da60  Node-1           1.0.5 192.168.4.50
```

To display AMF information for all nodes in the AMF, use the command:

```
node_1# show atmf nodes all
```

Table 43: Sample output from the **show atmf nodes all** command showing

```
node1#show atmf nodes all

Node and Guest Information:  * = Local device  SC = Switch Configuration:
  C = Chassis   S = Stackable   N = Standalone G = Guest

Node/Guest              Device              ATMF         Parent              Node
Name                    Type                Master  SC   Domain             Depth
-------------------------------------------------------------------------------
  x930-master           AT-x930-52GTX         Y     S    none                 0
* x510-master           x510-28GPX            Y     S    none                 0
  x908                  SwitchBlade x908      N     S    x510-master          1
  poe                   x610-48Ts/X-POE+      N     S    x908                 2
  aastra-phone          Aastra IP Phone       N     G    poe                  -
  poe-1.0.1                                   N     G    poe                  -
  ip-camera                                   N     G    poe                  -
  tq4600                AT-TQ4600             N     G    poe                  -
```

Related Commands

show atmf

show atmf area nodes

discovery

http-enable

show atmf backup guest

show atmf provision nodes

Overview This command displays information about each provisioned node with details about date and time of creation, boot and configuration files available in the backup, and license files present in the provisioned backup. This includes nodes that have joined the network but are yet to run their first backup.

This command can only be run on AMF master and controller nodes.

Syntax

```
show atmf provision nodes
```

Mode Privileged Exec

Usage This command will only work if provisioned nodes have already been set up. Otherwise, an error message is shown when the command is run.

Example To show the details of all the provisioned nodes in the backup use the command:

```
NodeName# show atmf provision nodes
```

Figure 40-17: Sample output from the **show atmf provision nodes** command

```
device1#show atmf provision nodes

ATMF Provisioned Node Information:

Backup Media .............: SD (Total 3827.0MB, Free 3481.1MB)

Node Name                 : device2
Date& Time                : 06-May-2014 & 23:25:44
Provision Path            : card:/atmf/provision_nodes

Boot configuration :
Current boot image        : x510-1766_atmf_backup.rel (file exists)
Backup  boot image        : x510-main-20140113-2.rel (file exists)
Default boot config       : flash:/default.cfg (file exists)
Current boot config       : flash:/abc.cfg (file exists)
Backup  boot config       : flash:/xyz.cfg (file exists)

Software Licenses :
Repository file           : ./.configs/.sw_v2.lic
                          : ./.configs/.swfeature.lic
Certificate file          : card:/atmf/nodes/awplus1/flash/.atmf-lic-cert
```

Related commands

atmf provision node create

atmf provision node clone

atmf provision node configure boot config

atmf provision node configure boot system

show atmf backup

show atmf tech

Overview This command collects and displays all the AMF command output. The command can thus be used to display a complete picture of an AMF network.

Syntax

```
show atmf tech
```

Mode Privileged Exec

Example To display output for all AMF commands, use the command:

```
NodeName# show atmf tech
```

Table 44: Sample output from the **show atmf tech** command.

```
node1#show atmf tech
ATMF Summary Information:

ATMF Status            : Enabled
Network Name           : ATMF_NET
Node Name              : node1
Role                   : Master
Current ATMF Nodes     : 8

ATMF Technical information:

Network Name                        : ATMF_NET
Domain                              : node1's domain
Node Depth                          : 0
Domain Flags                        : 0
Authentication Type                 : 0
MAC Address                         : 0014.2299.137d
Board ID                            : 287
Domain State                        : DomainController
Domain Controller                   : node1
Backup Domain Controller            : node2
Domain controller MAC               : 0014.2299.137d
Parent Domain                       : -
Parent Domain Controller            : -
Parent Domain Controller MAC        : 0000.0000.0000
Number of Domain Events             : 0
Crosslink Ports Blocking            : 0
Uplink Ports Waiting on Sync        : 0
```

Table 44: Sample output from the **show atmf tech** command. (cont.)

```
Crosslink Sequence Number          : 7
Domains Sequence Number            : 28
Uplink Sequence Number             : 2
Number of Crosslink Ports          : 1
Number of Domain Nodes             : 2
Number of Neighbors                : 5
Number of Non Broadcast Neighbors  : 3
Number of Link State Entries       : 1
Number of Up Uplinks               : 0
Number of Up Uplinks on This Node  : 0
DBE Checksum                       : 84fc6
Number of DBE Entries              : 0
...
```

Table 45: Parameter definitions from the **show atmf tech** command

Parameter	Definition
ATMF Status	Shows status of AMF feature on the Node as Enabled/Disabled.
Network Name	The name of the AMF network to which this node belongs.
Node Name	The name assigned to the node within the AMF network.
Role	The role configured on the device within the AMF - either master or member.
Current ATMF Nodes	A count of the AMF nodes in the AMF network.
Node Address	The identity of a node (in the format name.atmf) that enables its access it from a remote location.
Node ID	A unique identifier assigned to an AMF node.
Node Depth	The number of nodes in the path from this node to the core domain.
Domain State	A node's state within an AMF Domain - either controller or backup.
Recovery State	The AMF node recovery status. Indicates whether a node recovery is in progress on this device - either Auto, Manual, or None.
Management VLAN	The VLAN created for traffic between nodes of different domains (up/down links). VLAN ID - In this example VLAN 4092 is configured as the Management VLAN. Management Subnet - the Network prefix for the subnet. Management IP Address - the IP address allocated for this traffic. Management Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)

Table 45: Parameter definitions from the **show atmf tech** command (cont.)

Parameter	Definition
`Domain VLAN`	The VLAN assigned for traffic between Nodes of same domain (crosslink). VLAN ID - In this example VLAN 4091 is configured as the domain VLAN. Domain Subnet - the Subnet address used for this traffic. Domain IP Address - the IP address allocated for this traffic. Domain Mask - the Netmask used to create a subnet for this traffic 255.255.128.0 (= prefix /17)
`Device Type`	Shows the Product Series Name.
`ATMF Master`	Indicates the node's membership of the core domain (membership is indicated by Y)
`SC`	Shows switch configuration: • C - Chassis (such as SBx8100 series) • S - Stackable (VCS) • N - Standalone
`Parent`	A node that is connected to the present node's uplink, i.e. one layer higher in the hierarchy.
`Node Depth`	Shows the number of nodes in path from the current node to the Core domain.

NOTE: *The **show atmf tech** command can produce very large output. For this reason only the most significant terms are defined in this table.*

show atmf virtual-links

Overview This command displays a summary of all virtual links (L2TP tunnels) currently in the running configuration.

Syntax

```
show atmf virtual-links [macaddress]
```

Parameter	Description
`show`	Show running system information
`atmf`	The Allied Telesis Management Framework (AMF)
`virtual-links`	Virtual AMF links information.
`macaddr`	Virtual AMF links Mac Address.

Mode Privileged Exec

Example 1 To display AMF virtual links, use the command:

```
node_1# show atmf virtual-links
```

Table 46: Sample output from the **show atmf virtual-links** command.

```
ATMF Link Remote Information:

Local     Local           Local   Remote          Remote  Retries  State
Port      Ip              Id      Ip              Id
-------------------------------------------------------------------------
vlink1    192.0.2.33      1       192.168.1.1     2       0        Down
vlink2    192.0.2.65      2       192.168.2.0     3       0        Up
```

In the above example, a centrally located switch has the IP address space 192.0.2.x/24. It has two VLANs assigned the subnets 192.0.2.33 and 192.0.2.65 using the prefix /27. Each subnet connects to a virtual link. The first link has the IP address 192.168.1.1 and has a Local ID of 1. The second has the IP address 192.168.2.1 and has the Local ID of 2.

Example 2 To display AMF virtual links MAC address information, use the command:

```
node_1# show atmf virtual-links macaddr
```

Table 47: Sample output from the **show atmf virtual-links macaddr** command.

```
ATMF Link Remote Information:

ATMF Management Bridge Information:

Bridge: br-atmfmgmt

port no mac addr                is local?       ageing timer
  1     00:00:cd:27:c2:07       yes                0.00
```

Table 48: Parameter definitions from the **show atmf virtual-links** command output

Parameter	Definition
vlink1	The tunnel named vlink1, equivalent to an L2TP tunnel.
Local ID	The local ID of the virtual link. This matches the vlink<number>
State	The operational state of the vlink (either Up or Down). This state is always displayed once a vlink has been created.
mac addr	AMF virtual links terminate on an internal soft bridge. The “show atmf virtual-links macaddress” command displays MAC Address information.
is local ?	Indicates whether the MAC displayed is for a local or a remote device.
ageing timer	Indicates the current aging state for each MAC address.

show atmf working-set

Overview This command displays the nodes that form the current AMF working-set.

Syntax

```
show atmf working-set
```

Mode Privileged Exec

Example To show current members of the working-set, use the command:

```
ATMF_NETWORK[6]# show atmf working-set
```

Table 49: Sample output from the **show atmf working-set** command.

```
ATMF Working Set Nodes:

node1, node2, node3, node4, node5, node6

Working set contains 6 nodes
```

Related Commands

atmf working-set

show atmf

show atmf group

show debugging atmf

Overview This command shows the debugging modes status for AMF.

Syntax

```
show debugging atmf
```

Mode User Exec and Global Configuration

Example To display the AMF debugging status, use the command:

```
node_1# show debugging atmf
```

Figure 40-18: Sample output from the **show debugging atmf** command.

```
node1# show debugging atmf
ATMF debugging status:
ATMF arealink debugging is on
ATMF link debugging is on
ATMF crosslink debugging is on
ATMF database debugging is on
ATMF neighbor debugging is on
ATMF packet debugging is on
ATMF error debugging is on
```

Related Commands debug atmf packet

show debugging atmf packet

Overview This command shows details of AMF Packet debug command settings.

Syntax

```
show debugging atmf packet
```

Mode User Exec and Global Configuration

Example To display the AMF packet debugging status, use the command:

```
node_1# show debug atmf packet
```

Figure 40-19: Sample output from the **show debugging atmf packet** command.

```
ATMF packet debugging is on
=== ATMF Packet Debugging Parameters===
Node Name: x908
Port name: port1.1.1
Limit: 500 packets
Direction: TX
Info Level: Level 2
Packet Type Bitmap:
2. Crosslink Hello BPDU pkt with downlink domain info
3. Crosslink Hello BPDU pkt with uplink info
4. Down and up link Hello BPDU pkts
6. Stack hello unicast pkts
8. DBE request
9. DBE update
10. DBE bitmap update
```

Related Commands

debug atmf

debug atmf packet

show running-config atmf

Overview This command displays the running system information that is specific to AMF.

Syntax

```
show running-config atmf
```

Mode User Exec and Global Configuration

Example To display the current configuration of AMF, use the following commands:

```
node_1# show running-config atmf
```

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Related Commands show running-config

no debug all

switchport atmf-arealink remote-area

Overview This command enables you to configure a port or aggregator to be an AMF arealink. AMF arealinks are designed to operate between two nodes in different areas in an AMF network.

Use the **no** variant of this command to remove any AMF-arealink that may exist for the selected port or aggregated link.

This command is only available on AMF controllers and master nodes.

Syntax

```
switchport atmf-arealink remote-area <area-name> vlan <2-4094>
no switchport atmf-arealink
```

Parameter	Description
<area-name>	The name of the remote area that the port is connecting to.
<2-4094>	The VLAN ID for the link. This VLAN cannot be used for any other purpose, and the same VLAN ID must be used at each end of the link.

Default By default, no arealinks are configured

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage Run this command on the port or aggregator at both ends of the link.

Each area must have the area-name configured, and the same area password must exist on both ends of the link.

Running this command will automatically place the port or static aggregator into trunk mode (i.e. switchport mode trunk) and will synchronize the area information stored on the two nodes.

You can configure multiple arealinks between two area nodes, but only one arealink at any time will be in use. All other arealinks will block information, to prevent network storms.

Do not use a VCStack port as an AMF link, even if you have configured the port as a data port. During AMF recovery, these ports revert to their default state of being VCStack ports, so AMF cannot use them for recovery. Use a standard front-panel data port instead.

Example To make a switchport 1.2.1 an arealink to the *Auckland* area on VLAN 6, use the following commands

```
controller-1# configure terminal
controller-1(config)# interface port1.2.1
controller-1(config-if)# switchport atmf-arealink remote-area
Auckland vlan 6
```

Related Commands

atmf area

atmf area password

atmf virtual-link

show atmf links

switchport atmf-crosslink

Overview This command configures the selected port, statically aggregated link or dynamic channel group (LACP) to be an AMF crosslink. Running this command will automatically place the port or aggregator into trunk mode (i.e. **switchport mode trunk**).

The connection between two AMF masters must utilize a crosslink. Crosslinks are used to carry the AMF control information between master nodes. Multiple crosslinks can be configured between two master nodes, but only one crosslink can be active at any particular time. All other crosslinks between masters will be placed in the blocking state, in order to prevent broadcast storms.

Use the **no** variant of this command to remove any crosslink that may exist for the selected port or aggregated link.

Syntax
```
switchport atmf-crosslink
no switchport atmf-crosslink
```

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage Crosslinks can be used anywhere within an AMF network. They have the effect of separating the AMF network into separate domains.

Where this command is used, it is also good practice to use the switchport trunk native vlan command with the parameter **none** selected. This is to prevent a network storm on a topology of ring connected devices.

Do not use a VCStack port as an AMF link, even if you have configured the port as a data port. During AMF recovery, these ports revert to their default state of being VCStack ports, so AMF cannot use them for recovery. Use a standard front-panel data port instead.

Example 1 To make a switchport 1.0.1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-crosslink
```

Example 2 This example is shown twice. Example 2A is the most basic command sequence. Example 2B is a good practice equivalent that avoids problems such as broadcast storms that can otherwise occur.

Example 2A To make static aggregator sa1 an AMF crosslink, use the following commands:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
```

Example 2B To make static aggregator sa1 an AMF crosslink, use the following commands for good practice:

```
Node_1# configure terminal
Node_1(config)# interface sa1
Node_1(config-if)# switchport atmf-crosslink
Node_1(config-if)# switchport trunk allowed vlan add 2
Node_1(config-if)# switchport trunk native vlan none
```

In this example VLAN 2 is assigned to the static aggregator, and the native VLAN (VLAN 1) is explicitly excluded from the aggregated ports and the crosslink assigned to it.

NOTE: *The AMF management and domain VLANs are automatically added to the aggregator and the crosslink.*

Related Commands show atmf links statistics

switchport atmf-guestlink

Overview Guest links are used to provide basic AMF functionality to non AMF capable devices. Guest links can be configured for either a selected switch port or a range of switch ports and use generic protocols to collect status and configuration information that the guest devices make available.

Use the **no** variant of this command to remove the guest node functionality from the selected port or ports.

Syntax

```
switchport atmf-guestlink [class <GUEST-CLASS>] [ip <A.B.C.D> | ipv6 <X:X::X:X>]
no switchport atmf-guestlink
```

Parameter	Description
`class`	Set a Guest-class
<GUEST-CLASS>	The name of the guest class.
`ip`	Specifies that the address following will have an IPv4 format
<A.B.C.D>	The Guest-node's IP address in IPv4 format.
`ipv6`	Specifies that the address following will have an IPv6 format
<X:X::X:X>	The Guest-node's IP address in IPv6 format.

Default No guest links are configured.

Mode Interface

Example 1 To configure switch port 1.0.44 to be a guest link, that will connect to a guest node having a guest-class of **camera** and an IPv4 address of **192.168.3.3**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.44
node1(config-if)# switchport atmf-guestlink class camera ip 192.168.3.3
node1(config-if)# end
```

Example 2 To configure switchport 1.0.41 to be a guest link, that will connect to a guest node having a guest-class of **phone** and an IPv6 address of **2001:db8:21e:10d::5**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.41
node1(config-if)# switchport atmf-guestlink class phone ipv6 2000:db8:21e:10d::5
node1(config-if)# end
```

Example 3 To configure switch port 1.0.41 to be a guest link, using the default model type and learning method address, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.41
node1(config-if)# switchport atmf-guestlink
node1(config-if)# end
```

Example 4 To configure switch ports 1.0.52 to 1.0.54 to be guest links, for the guest class **camera**, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.41-port1.0.44
node1(config-if)# switchport atmf-guestlink class camera
node1(config-if)# end
```

Example 5 To remove the guest-link functionality from switchport 1.0.41, use the following commands:

```
node1# configure terminal
node1(config)# int port1.0.41
node1(config-if)# no switchport atmf-guestlink
node1(config-if)# end
```

Related Commands

atmf guest-class

discovery

http-enable

username

modeltype

show atmf links guest

show atmf guest

switchport atmf-link

Overview This command enables you to configure a port or aggregator to be an AMF uplink/downlink. Running this command will automatically place the port or aggregator into trunk mode.

Use the **no** variant of this command to remove any AMF-link that may exist for the selected port or aggregated link.

Syntax

```
switchport atmf-link
no switchport atmf-link
```

Mode Interface Configuration for a switchport, a static aggregator or a dynamic channel group.

Usage Do not use a VCStack port as an AMF link, even if you have configured the port as a data port. During AMF recovery, these ports revert to their default state of being VCStack ports, so AMF cannot use them for recovery. Use a standard front-panel data port instead.

Example To make a switchport 1.0.1 an AMF uplink/downlink, use the following commands

```
Node_1# configure terminal
Node_1(config)# interface port1.0.1
Node_1(config-if)# switchport atmf-link
```

type atmf node

Overview This command configures a trigger to be activated at an AMF node join event or leave event.

Syntax

```
type atmf node {join|leave}
```

Parameter	Description
join	AMF node join event.
leave	AMF node leave event.

Mode Trigger Configuration

CAUTION: *Only configure this trigger on one device because it is a network wide event.*

Example 1 To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
========

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------

==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related Commands show trigger

undebug atmf

Overview This command is an alias for the **no** variant of the debug atmf command.

username

Overview This command enables you to assign a **username** to a guest class. Guests may require a username and possibly also a password. In its non-encypted form the password must be between 1 and 32 characters and will allow spaces. In its encrypted form the password must be between 1 to 64 characters and will allow any character

Syntax

```
username <NAME> password [8] <USERPASS>
no username
```

Parameter	Description
`username`	Indicates that a user name is to follow
<NAME>	User name of the guest node
`password`	Indicates that a password (or specifier) is to follow.
`8`	Specifier indicating that the following password is encrypted. It's primary purpose is to differentiate between the configuration input and the CLI input. You should not specify this for CLI input
<USERPASS>	The password to be entered for the guest node.

Default No usernames configured

Mode AMF Guest Configuration Mode

Example 1 To assign the user name **reception** and the password of **secret** to an AMF guest node that has the guest class of **phone1** use the following commands:

```
node1# conf t
node1(config)# amf guest-class phone1
node1(config-atmf-guest)# username reception password secret
node1(config-atmf-guest)# end
```

Example 2 To remove a guest node username and password for the user guest class **phone1**, use the following commands:

```
node1# conf t
node1(config)# atmf guest-class phone1
node1(config-atmf-guest)# no username
node1(config-atmf-guest)# end
```

Related Commands

show atmf links detail

atmf guest-class

switchport atmf-guestlink

41 Dynamic Host Configuration Protocol (DHCP) Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure DHCP.

For more information, see the DHCP Feature Overview and Configuration Guide, which is available at the above link on alliedtelesis.com.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide. This guide is available at the above link on alliedtelesis.com.

Command List

bootfile

Overview This command sets the boot filename for a DHCP server pool. This is the name of the boot file that the client should use in its bootstrap process. It may need to include a path.

The **no** variant of this command removes the boot filename from a DHCP server pool.

Syntax

```
bootfile <filename>
no bootfile
```

Parameter	Description
<filename>	The boot file name.

Mode DHCP Configuration

Example To configure the boot filename for a pool `P2`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# bootfile boot/main_boot.bt
```

clear ip dhcp binding

Overview This command clears either a specific lease binding or the lease bindings specified by the command or DHCP server. The command will only take effect on dynamically allocated bindings, not statically configured bindings.

Syntax

```
clear ip dhcp binding {ip <ip-address>|mac
<mac-address>|all|pool <pool-name>|range <low-ip-address>
<high-ip-address>}
```

Parameter	Description
`ip <ip-address>`	IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D.
`mac <mac-address>`	MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH.
`all`	All DHCP bindings.
`pool <pool-name>`	Description used to identify DHCP server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in “quotation marks”.
`range<low-ip-address> <high-ip-address>`	IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end of the range.

Mode User Exec and Privileged Exec

Usage A specific binding may be deleted by **ip** address or **mac** address, or several bindings may be deleted at once using **all**, **pool** or **range**.

Note that if you specify to clear the **ip** or **mac** address of what is actually a static DHCP binding, an error message is displayed. If **all**, **pool** or **range** are specified and one or more static DHCP bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

Examples To clear the specific IP address binding `192.168.1.1`, use the command:

```
awplus# clear ip dhcp binding ip 192.168.1.1
```

To clear all dynamic DHCP entries, use the command:

```
awplus# clear ip dhcp binding all
```

Related Commands show ip dhcp binding

default-router

Overview This command adds a default router to the DHCP address pool you are configuring. You can use this command multiple times to create a list of default routers on the client's subnet. This sets the router details using the pre-defined option 3. Note that if you add a user-defined option 3 using the **option** command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified default router, or all default routers from the DHCP pool.

Syntax

```
default-router <ip-address>
no default-router [<ip-address>]
```

Parameter	Description
<ip-address>	IPv4 address of the default router, in dotted decimal notation.

Mode DHCP Configuration

Examples To add a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# default-router 192.168.1.2
```

To remove a router with an IP address 192.168.1.2 to the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router 192.168.1.2
```

To remove all routers from the DHCP pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no default-router
```

dns-server

Overview This command adds a Domain Name System (DNS) server to the DHCP address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6.

Note that if you add a user-defined option 6 using the option command, then you will override any settings created with this command.

The **no** variant of this command removes either the specified DNS server, or all DNS servers from the DHCP pool.

Syntax

```
dns-server <ip-address>
no dns-server [<ip-address>]
```

Parameter	Description
<ip-address>	IPv4 address of the DNS server, in dotted decimal notation.

Mode DHCP Configuration

Examples To add the DNS server with the assigned IP address 192.168.1.1 to the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# dns-server 192.168.1.1
```

To remove the DNS server with the assigned IP address 192.168.1.1 from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server 192.168.1.1
```

To remove all DNS servers from the DHCP pool named P1, use the following commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no dns-server
```

Related Commands

default-router

option

service dhcp-server

show ip dhcp pool

subnet-mask

domain-name

Overview This command adds a domain name to the DHCP address pool you are configuring. Use this command to specify the domain name that a client should use when resolving host names using the Domain Name System. This sets the domain name details using the pre-defined option 15.

Note that if you add a user-defined option 15 using the option command, then you will override any settings created with this command.

The **no** variant of this command removes the domain name from the address pool.

Syntax

```
domain-name <domain-name>
no domain-name
```

Parameter	Description
<domain-name>	The domain name you wish to assign the DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".

Mode DHCP Configuration

Examples To add the domain name `Nerv_Office` to DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# domain-name Nerv_Office
```

To remove the domain name `Nerv_Office` from DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no domain-name Nerv_Office
```

Related Commands

default-router

dns-server

option

service dhcp-server

show ip dhcp pool

subnet-mask

host (DHCP)

Overview This command adds a static host address to the DHCP address pool you are configuring. The client with the matching MAC address is permanently assigned this IP address. No other clients can request it.

The **no** variant of this command removes the specified host address from the DHCP pool. Use the **no host all** command to remove all static host addresses from the DHCP pool.

Syntax

```
host <ip-address> <mac-address>
no host <ip-address>
no host all
```

Parameter	Description
<ip-address>	IPv4 address of the DHCP client, in dotted decimal notation in the format A.B.C.D
<mac-address>	MAC address of the DHCP client, in hexadecimal notation in the format HHHH.HHHH.HHHH

Mode DHCP Configuration

Usage Note that a network/mask must be configured using a **network** command before issuing a **host** command. Also note that a host address must match a network to add a static host address.

Examples To add the host at `192.168.1.5` with the MAC address `000a.451d.6e34` to DHCP pool `1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# network 192.168.1.0/24
awplus(dhcp-config)# host 192.168.1.5 000a.451d.6e34
```

To remove the host at `192.168.1.5` with the MAC address `000a.451d.6e34` from DHCP pool `1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool 1
awplus(dhcp-config)# no host 192.168.1.5 000a.451d.6e34
```

Related Commands

lease

range

show ip dhcp pool

ip address dhcp

Overview This command activates the DHCP client on the interface you are configuring. This allows the interface to use the DHCP client to obtain its IP configuration details from a DHCP server on its connected network.

The **client-id** and **hostname** parameters are identifiers that you may want to set in order to interoperate with your existing DHCP infrastructure. If neither option is needed, then the DHCP server uses the MAC address field of the request to identify the host.

The DHCP client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 3 - a list of default routers.
- Option 6 - a list of DNS servers. This list appends the DNS servers set on your device with the ip name-server command.
- Option 15 - a domain name used to resolve host names. This option replaces the domain name set with the ip domain-name command. Your device ignores this domain name if it has a domain list set using the ip domain-list command.
- Option 51 - lease expiration time.

The **no** variant of this command stops the interface from obtaining IP configuration details from a DHCP server.

Syntax

```
ip address dhcp [client-id <interface>] [hostname <hostname>]
no ip address dhcp
```

Parameter	Description
<interface>	The name of the interface you are activating the DHCP client on. If you specify this, then the MAC address associated with the specified interface is sent to the DHCP server in the optional identifier field. Default: no default
<hostname>	The hostname for the DHCP client on this interface. Typically this name is provided by the ISP. Default: no default

Mode Interface Configuration for a VLAN interface.

Examples To set the interface vlan10 to use DHCP to obtain an IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip address dhcp
```

To stop the interface vlan10 from using DHCP to obtain its IP address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip address dhcp
```

Related Commands

ip address (IP Addressing and Protocol)

show ip interface

show running-config

ip dhcp bootp ignore

Overview This command configures the DHCP server to ignore any BOOTP requests it receives. The DHCP server accepts BOOTP requests by default.

The **no** variant of this command configures the DHCP server to accept BOOTP requests. This is the default setting.

Syntax

```
ip dhcp bootp ignore
no ip dhcp bootp ignore
```

Mode Global Configuration

Examples To configure the DHCP server to ignore BOOTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp bootp ignore
```

To configure the DHCP server to respond to BOOTP requests, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp bootp ignore
```

Related Commands show ip dhcp server summary

ip dhcp leasequery enable

Overview Use this command to enable the DHCP server to respond to DHCPLEASEQUERY packets. Enabling the DHCP leasequery feature allows a DHCP Relay Agent to obtain IP address information directly from the DHCP server using DHCPLEASEQUERY messages.

Use the **no** variant of this command to disable the support of DHCPLEASEQUERY packets.

For more information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp leasequery enable
no ip dhcp leasequery enable
```

Default DHCP leasequery support is disabled by default.

Mode Global Configuration

Examples To enable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp leasequery enable
```

To disable DHCP leasequery support, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp leasequery enable
```

Related Commands

show counter dhcp-server

show ip dhcp server statistics

show ip dhcp server summary

ip dhcp option

Overview This command creates a user-defined DHCP option. Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

You can use this option when configuring a DHCP pool, by using the option command.

The **no** variant of this command removes either the specified user-defined option, or removes all user-defined options. This also automatically removes the user-defined options from the associated DHCP address pools.

Syntax

```
ip dhcp option <1-254> [name <option-name>] [<option-type>]
no ip dhcp option [<1-254>|<option-name>]
```

Parameter	Description	
<1-254>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.	
<option-name>	Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”. Default: no default	
<option-type>	The option value. You must specify a value that is appropriate to the option type:	
	`asci`	An ASCII text string
	`hex`	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	`ip`	An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually by using the option command multiple times.
	`integer`	A number from 0 to 4294967295.
	`flag`	A value that either sets (to 1) or unsets (to 0) a flag: **true**, **on**, or **enabled** will set the flag. **f alse**, **off** or **disabled** will unset the flag.

Mode Global Configuration

Examples

To define a user-defined ASCII string option as option 66, without a name, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name "tcpip-node-type", use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name `special-address`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number `12`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option 12
```

To remove the specific user-defined option with the option name `perform-router-discovery`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option perform-router-discovery
```

To remove all user-defined option definitions, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp option
```

Related Commands

default-router

dns-server

domain-name

option

service dhcp-server

show ip dhcp server summary

subnet-mask

ip dhcp pool

Overview This command will enter the configuration mode for the pool name specified. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCP configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCP pools on devices with multiple interfaces. This allows the device to act as a DHCP server on multiple interfaces to distribute different information to clients on the different networks.

The **no** variant of this command deletes the specific DHCP pool.

Syntax

```
ip dhcp pool <pool-name>
no ip dhcp pool <pool-name>
```

Parameter	Description
<pool-name>	Description used to identify this DHCP pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”.

Mode Global Configuration

Example To create the DHCP pool named `P2` and enter DHCP Configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)#
```

To delete the DHCP pool named `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# no ip dhcp pool P2
```

Related Commands service dhcp-server

ip dhcp-relay agent-option

Overview This command enables the DHCP Relay Agent to insert the DHCP Relay Agent Information Option (Option 82) into the client-request packets that it relays to its DHCP server. This allows the DHCP Relay Agent to pass on information to the server about the network location of the client device. The DHCP Relay Agent strips the DHCP Relay Agent Option 82 field out of the DHCP server's response, so that the DHCP client never sees this field.

When the DHCP Relay Agent appends its DHCP Relay Agent Option 82 data into the packet, it first overwrites any pad options present; then if necessary, it increases the packet length to accommodate the DHCP Relay Agent Option 82 data.

The **no** variant of this command stops the DHCP Relay Agent from appending the Option 82 field onto DHCP requests before forwarding it to the server.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

NOTE: *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands ip dhcp-relay agent-option and ip dhcp-relay information policy have been configured.*

Syntax

```
ip dhcp-relay agent-option
no ip dhcp-relay agent-option
```

Default DHCP Relay Agent Information Option (Option 82) insertion is disabled by default.

Mode Interface Configuration for a VLAN interface.

Usage Use this command to alter the DHCP Relay Agent Option 82 setting when your device is the first hop for the DHCP client. To limit the maximum length of the packet, use the ip dhcp-relay max-message-length command.

This command cannot be enabled if DHCP snooping is enabled on your device (service dhcp-snooping command), and vice versa.

Examples To make the DHCP Relay Agent listening on `vlan15` append the DHCP Relay Agent Option 82 field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay agent-option
```

To stop the DHCP Relay Agent from appending the DHCP Relay Agent Option 82 field on `vlan15`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# no ip dhcp-relay agent-option
```

Related Commands

ip dhcp-relay agent-option remote-id

ip dhcp-relay information policy

ip dhcp-relay max-message-length

service dhcp-relay

ip dhcp-relay agent-option checking

Overview

This command enables the DHCP Relay Agent to check DHCP Relay Agent Information Option (Option 82) information in response packets returned from DHCP servers. If the information does not match the information it has for its own client (downstream) interface then the DHCP Relay Agent drops the packet. Note that ip dhcp-relay agent-option must be configured.

The DHCP Relay Agent Option 82 field is included in relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (ip dhcp-relay agent-option), and
- DHCP Relay Agent is enabled on the device (service dhcp-relay)

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay agent-option checking
no ip dhcp-relay agent-option checking
```

Mode

Interface Configuration for a VLAN interface.

Examples

To make the DHCP Relay Agent listening on vlan10 check the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# ip dhcp-relay agent-option
awplus(config-if)# ip dhcp-relay agent-option checking
```

To stop the DHCP Relay Agent on vlan10 from checking the DHCP Relay Agent Information Option (Option 82) field, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay agent-option checking
```

Related Commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option remote-id

ip dhcp-relay information policy

service dhcp-relay

ip dhcp-relay agent-option remote-id

Overview Use this command to specify the Remote ID sub-option of the DHCP Relay Agent Option 82 field the DHCP Relay Agent inserts into clients' request packets. The Remote ID identifies the device that is inserting the DHCP Relay Agent Option 82 information. If a Remote ID is not specified, the Remote ID sub-option is set to the device's MAC address.

Use the **no** variant of this command to return the Remote ID for an interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay agent-option remote-id <remote-id>
no ip dhcp-relay agent-option remote-id
```

Parameter	Description
<remote-id>	An alphanumeric (ASCII) string, 1 to 63 characters in length. Additional characters allowed are hyphen (-), underscore (_) and hash (#). Spaces are not allowed.

Default The Remote ID is set to the device's MAC address by default.

Mode Interface Configuration for a VLAN interface.

Usage The Remote ID sub-option is included in the DHCP Relay Agent Option 82 field of relayed client DHCP packets if:

- DHCP Relay Agent Option 82 is enabled (ip dhcp-relay agent-option), and
- DHCP Relay Agent is enabled on the device (service dhcp-relay)

Examples To set the Remote ID to `myid` for client DHCP packets received on `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ip dhcp-relay agent-option remote-id myid
```

To remove the Remote ID specified for `vlan1`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# no ip dhcp-relay agent-option remote-id
```

Related Commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

show ip dhcp-relay

ip dhcp-relay information policy

Overview This command sets the policy for how the DHCP relay deals with packets arriving from the client that contain DHCP Relay Agent Option 82 information.

If the command **ip dhcp-relay agent-option** has not been configured, then this command has no effect at all - no alteration is made to Option 82 information in packets arriving from the client side.

However, if the command **ip dhcp-relay agent-option** has been configured, this command modifies how the DHCP relay service deals with cases where the packet arriving from the client side already contains DHCP Relay Agent Option 82 information.

This command sets the action that the DHCP relay should take when a received DHCP client request contains DHCP Relay Agent Option 82 information.

By default, the DHCP Relay Agent replaces any existing DHCP Relay Agent Option 82 field with its own DHCP Relay Agent field. This is equivalent to the functionality of the **replace** parameter.

The **no** variant of this command returns the policy to the default behavior - i.e. replacing the existing DHCP Relay Agent Option 82 field.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

NOTE: *The DHCP-relay service might alter the content of the DHCP Relay Agent Option 82 field, if the commands ip dhcp-relay agent-option and ip dhcp-relay information policy have been configured.*

Syntax

```
ip dhcp-relay information policy {append|drop|keep|replace}
no ip dhcp-relay information policy
```

Parameter	Description
`append`	The DHCP Relay Agent appends the DHCP Relay Agent Option 82 field of the packet with its own DHCP Relay Agent Option 82 details.
`drop`	The DHCP Relay Agent discards the packet.
`keep`	The DHCP Relay Agent forwards the packet without altering the DHCP Relay Agent Option 82 field.
`replace`	The DHCP Relay Agent replaces the existing DHCP Relay Agent details in the DHCP Relay Agent Option 82 field with its own details before forwarding the packet.

Mode Interface Configuration for a VLAN interface.

Examples

To make the DHCP Relay Agent listening on `vlan15` drop any client requests that already contain DHCP Relay Agent Option 82 information, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay information policy drop
```

To reset the DHCP relay information policy to the default policy for interface `vlan15`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# no ip dhcp-relay information policy
```

Related Commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

service dhcp-server

ip dhcp-relay maxhops

Overview This command sets the hop count threshold for discarding BOOTP messages. When the hops field in a BOOTP message exceeds the threshold, the DHCP Relay Agent discards the BOOTP message. The hop count threshold is set to 10 hops by default.

Use the **no** variant of this command to reset the hop count to the default.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay maxhops <1-255>
no ip dhcp-relay maxhops
```

Parameter	Description
<1-255>	The maximum hop count value.

Default The default hop count threshold is 10 hops.

Mode Interface Configuration for a VLAN interface.

Example To set the maximum number of hops to 5 for packets received on interface `vlan15`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan15
awplus(config-if)# ip dhcp-relay maxhops 5
```

Related Commands service dhcp-relay

ip dhcp-relay max-message-length

Overview This command applies when the device is acting as a DHCP Relay Agent and DHCP Relay Agent Option 82 insertion is enabled. It sets the maximum DHCP message length (in bytes) for the DHCP packet with its DHCP Relay Agent Option 82 data inserted. From this value it calculates the maximum packet size that it will accept at its input. Packets that arrive greater than this value will be dropped.

The **no** variant of this command sets the maximum message length to its default of 1400 bytes.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay max-message-length <548-1472>
no ip dhcp-relay max-message-length
```

Parameter	Description
<548-1472>	The maximum DHCP message length (this is the message header plus the inserted DHCP option fields in bytes).

Default The default is 1400 bytes.

Mode Interface Configuration for a VLAN interface.

Usage When a DHCP Relay Agent (that has DHCP Relay Agent Option 82 insertion enabled) receives a request packet from a DHCP client, it will append the DHCP Relay Agent Option 82 component data, and forward the packet to the DHCP server. The DHCP client will sometimes issue packets containing pad option fields that can be overwritten with Option 82 data.

Where there are insufficient pad option fields to contain all the DHCP Relay Agent Option 82 data, the DHCP Relay Agent will increase the packet size to accommodate the DHCP Relay Agent Option 82 data. If the new (increased) packet size exceeds that defined by the **maximum-message-length** parameter, then the DHCP Relay Agent will drop the packet.

NOTE: *Before setting this command, you must first run the ip dhcp-relay agent-option command. This will allow the DHCP Relay Agent Option 82 fields to be appended.*

Example To set the maximum DHCP message length to 1200 bytes for packets arriving in interface `vlan7`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# ip dhcp-relay max-message-length 1200
```

To reset the maximum DHCP message length to the default of 1400 bytes for packets arriving in interface `vlan7`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan7
awplus(config-if)# no ip dhcp-relay max-message-length
```

Related Commands service dhcp-relay

ip dhcp-relay server-address

Overview This command adds a DHCP server for the DHCP Relay Agent to forward client DHCP packets to on a particular interface. You can add up to five DHCP servers on each device interface that the DHCP Relay Agent is listening on.

The **no** variant of this command deletes the specified DHCP server from the list of servers available to the DHCP relay agent.

The **no ip dhcp-relay** command removes all DHCP relay settings from the interface.

For DHCP Relay Agent and DHCP Relay Agent Option 82 introductory information, see the DHCP Feature Overview and Configuration Guide.

Syntax

```
ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}
no ip dhcp-relay server-address {<ipv4-address>|<ipv6-address>
<server-interface>}
no ip dhcp-relay
```

Parameter	Description
<ipv4-address>	Specify the IPv4 address of the DHCP server for DHCP Relay Agent to forward client DHCP packets to, in dotted decimal notation. The IPv4 address uses the format A.B.C.D.
<ipv6-address>	Specify the IPv6 address of the DHCPv6 server for DHCPv6 Relay Agent to forward client DHCP packets to, in hexadecimal notation.
<server-interface>	Specify the interface name of the DHCPv6 server. It is only required for a DHCPv6 server with an IPv6 address.

Mode Interface Configuration for a VLAN interface.

Usage For a DHCP server with an IPv6 address you must specify the interface for the DHCP server. See examples below for configuration differences between IPv4 and IPv6 DHCP relay servers.

See also the service dhcp-relay command to enable the DHCP Relay Agent on your device. The ip dhcp-relay server-address command defines a relay destination on an interface on the device, needed by the DHCP Relay Agent to relay DHCP client packets to a DHCP server.

Examples

To enable the DHCP Relay Agent to relay DHCP packets on interface `vlan2` to the DHCP server with the IPv4 address `192.0.2.200`, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan2
awplus(config-if)# ip dhcp-relay server-address 192.0.2.200
```

To remove the DHCP server with the IPv4 address `192.0.2.200` from the list of servers available to the DHCP Relay Agent on interface `vlan2`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ip dhcp-relay server-address 192.0.2.200
```

To enable the DHCP Relay Agent on your device to relay DHCP packets on interface `vlan10` to the DHCP server with the IPv6 address `2001:0db8:010d::1` on interface `vlan20`, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
awplus(config)# interface vlan10
awplus(config-if)# ip dhcp-relay server-address
2001:0db8:010d::1 vlan20
```

To remove the DHCP server with the IPv6 address `2001:0db8:010d::1` on interface `vlan20` from the list of servers available to the DHCP Relay Agent on interface `vlan10`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay server-address
2001:0db8:010d::1 vlan20
```

To disable DHCP relay on `vlan10`, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ip dhcp-relay
```

Related Commands

service dhcp-relay

lease

Overview This command sets the expiration time for a leased address for the DHCP address pool you are configuring. The time set by the days, hours, minutes and seconds is cumulative. The minimum total lease time that can be configured is 20 seconds. The maximum total lease time that can be configured is 120 days.

Note that if you add a user-defined option 51 using the option command, then you will override any settings created with this command. Option 51 specifies a lease time of 1 day.

Use the **infinite** parameter to set the lease expiry time to infinite (leases never expire).

Use the **no** variant of this command to return the lease expiration time back to the default of one day.

Syntax

```
lease <days> <hours> <minutes> [<seconds>]
lease infinite
no lease
```

Parameter	Description
<days>	The number of days, from 0 to 120, that the lease expiry time is configured for. Default: 1
<hours>	The number of hours, from 0 to 24, that the lease expiry time is configured for. Default: 0
<minutes>	The number of minutes, from 0 to 60, the lease expiry time is configured for. Default: 0
<seconds>	The number of seconds, from 0 to 60, the lease expiry time is configured for.
`infinite`	The lease never expires.

Default The default lease time is 1 day.

Mode DHCP Configuration

Examples To set the lease expiration time for address pool `P2` to 35 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# lease 0 0 35
```

To set the lease expiration time for the address pool `Nerv_Office` to 1 day, 5 hours, and 30 minutes, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# lease 1 5 30
```

To set the lease expiration time for the address pool `P3` to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P3
awplus(dhcp-config)# lease 0 0 0 20
```

To set the lease expiration time for the pool to never expire, use the command:

```
awplus(dhcp-config)# lease infinite
```

To return the lease expiration time to the default of one day, use the command:

```
awplus(dhcp-config)# no lease
```

Related Commands

option

service dhcp-server

network (DHCP)

Overview This command sets the network (subnet) that the DHCP address pool applies to.

The **no** variant of this command removes the network (subnet) from the DHCP address pool.

Syntax

```
network
{<ip-subnet-address/prefix-length>|<ip-subnet-address/mask>}
no network
```

Parameter	Description
<ip-subnet-address/prefix-length>	The IPv4 subnet address in dotted decimal notation followed by the prefix length in slash notation.
<ip-subnet-address/mask>	The IPv4 subnet address in dotted decimal notation followed by the subnet mask in dotted decimal notation.

Mode DHCP Configuration

Usage This command will fail if it would make existing ranges invalid. For example, if they do not lie within the new network you are configuring.

The **no** variant of this command will fail if ranges still exist in the pool. You must remove all ranges in the pool before issuing a **no network** command to remove a network from the pool.

Examples To configure a network for the address pool `P2`, where the subnet is `192.0.2.5` and the mask is `255.255.255.0`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5/24
```

or you can use dotted decimal notation instead of slash notation for the subnet-mask:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# network 192.0.2.5 255.255.255.0
```

Related Commands service dhcp-server

subnet-mask

next-server

Overview This command sets the next server address for a DHCP server pool. It is the address of the next server that the client should use in its bootstrap process.

The **no** variant of this command removes the next server address from the DHCP address pool.

Syntax

```
next-server <ip-address>
no next-server
```

Parameter	Description
<ip-address>	The server IP address, entered in dotted decimal notation.

Mode DHCP Configuration

Example To set the next-server address for the address pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# next-server 192.0.2.2
```

option

Overview This command adds a user-defined option to the DHCP address pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value. Options with an **ip** type can hold a list of IP addresses or masks (i.e. entries that have the A.B.C.D address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IP addresses.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

The **no** variant of this command removes the specified user-defined option from the DHCP pool, or all user-defined options from the DHCP pool.

Syntax

```
option [<1-254>|<option-name>] <option-value>
no option [<1-254>|<option-value>]
```

Parameter	Description	
<1-254>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.	
<option-name>	Option name associated with the option.	
<option-value>	The option value. You must specify a value that is appropriate to the option type:	
	`hex`	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	`ip`	An IPv4 address or mask that has the dotted decimal A.B.C.D notation. To create a list of IP addresses, you must add each IP address individually using the option command multiple times.
	`integer`	A number from 0 to 4294967295.
	`flag`	A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.

Mode DHCP Configuration

Examples

To add the ASCII-type option named `tftp-server-name` to the pool `P2` and give the option the value `server1`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tftp-server-name server1
```

To add the hex-type option named `tcpip-node-type` to the pool `P2` and give the option the value `08af`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option `175`, use the command:

```
awplus(dhcp-config)# option 175 192.0.2.6
awplus(dhcp-config)# option 175 192.0.2.12
awplus(dhcp-config)# option 175 192.0.2.33
```

To add the option `179` to a pool, and give the option the value `123456`, use the command:

```
awplus(dhcp-config)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the command:

```
awplus(dhcp-config)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the command:

```
awplus(dhcp-config)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the command:

```
awplus(dhcp-config)# no option tftp-server-name
```

Related Commands

dns-server

ip dhcp option

lease

service dhcp-server

show ip dhcp pool

probe enable

Overview Use this command to enable lease probing for a DHCP pool. Probing is used by the DHCP server to check if an IP address it wants to lease to a client is already being used by another host.

The **no** variant of this command disables probing for a DHCP pool.

Syntax

```
probe enable
no probe enable
```

Default Probing is enabled by default.

Mode DHCP Pool Configuration

Examples To enable probing for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe enable
```

To disable probing for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe enable
```

Related Commands

ip dhcp pool

probe packets

probe timeout

probe type

show ip dhcp pool

probe packets

Overview Use this command to specify the number of packets sent for each lease probe. Lease probing is configured on a per-DHCP pool basis. When set to 0 probing is effectively disabled.

The **no** variant of this command sets the number of probe packets sent to the default of 5.

Syntax

```
probe packets <0-10>
no probe packets
```

Parameter	Description
<0-10>	The number of probe packets sent.

Default The default is 5.

Mode DHCP Pool Configuration

Examples To set the number of probe packets to 2 for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe packets 2
```

To set the number of probe packets to the default 5 for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe packets
```

Related Commands

probe enable

probe timeout

probe type

show ip dhcp pool

probe timeout

Overview Use this command to set the timeout value in milliseconds that the server waits for a response after each probe packet is sent. Lease probing is configured on a per-DHCP pool basis.

The **no** variant of this command sets the probe timeout value to the default setting, 200 milliseconds.

Syntax

```
probe timeout <50-5000>
no probe timeout
```

Parameter	Description
<50-5000>	Timeout interval in milliseconds.

Default The default timeout interval is 200 milliseconds.

Mode DHCP Pool Configuration

Examples To set the probe timeout value to 500 milliseconds for pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe timeout 500
```

To set the probe timeout value for pool `P2` to the default, 200 milliseconds, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe timeout
```

Related Commands

probe enable

probe packets

probe type

show ip dhcp pool

probe type

Overview Use this command to set the probe type for a DHCP pool. The probe type specifies how the DHCP server checks whether an IP address is being used by other hosts, referred to as lease probing. If **arp** is specified, the server sends an ARP request to determine if an address is in use. If **ping** is specified, the server will send an ICMP Echo Request (ping).

The **no** variant of this command sets the probe type to the default setting, ping.

Syntax

```
probe type {arp|ping}
no probe type
```

Parameter	Description
`arp`	Probe using ARP.
`ping`	Probe using ping.

Default The default probe type is ping.

Mode DHCP Pool Configuration

Examples To set the probe type to `arp` for the pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# probe type arp
```

To set the probe type for the pool `P2` to the default, `ping`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no probe type
```

Related Commands

ip dhcp pool

probe enable

probe packets

probe timeout

show ip dhcp pool

range

Overview This command adds an address range to the DHCP address pool you are configuring. The DHCP server responds to client requests received from the pool's network. It assigns an IP addresses within the specified range. The IP address range must lie within the network. You can add multiple address ranges and individual IP addresses for a DHCP pool by using this command multiple times.

The **no** variant of this command removes an address range from the DHCP pool. Use the **no range all** command to remove all address ranges from the DHCP pool.

Syntax

```
range <ip-address> [<ip-address>]
no range <ip-address> [<ip-address>]
no range all
```

Parameter	Description
<ip-address>	IPv4 address range for DHCP clients, in dotted decimal notation. The first IP address is the low end of the range, the second IP address is the high end. Specify only one IP address to add an individual IP address to the address pool.

Mode DHCP Configuration

Examples To add an address range of `192.0.2.5` to `192.0.2.16` to the pool `Nerv_Office`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool Nerv_Office
awplus(dhcp-config)# range 192.0.2.5 192.0.2.16
```

To add the individual IP address `192.0.2.2` to a pool, use the command:

```
awplus(dhcp-config)# range 192.0.2.2
```

To remove all address ranges from a pool, use the command:

```
awplus(dhcp-config)# no range all
```

Related Commands

ip dhcp pool

service dhcp-server

show ip dhcp pool

route

Overview This command allows the DHCP server to provide static routes to clients.

Syntax

```
route A.B.C.D/M A.B.C.D {both|opt249|rfc3442}
```

Parameter	Description
`A.B.C.D/M`	Subnet for the route
`A.B.C.D`	Next hop for the route
`both`	opt249 and rft3442
`opt249`	Classless static route option for DHCP
`rfc3442`	Classless static route option for DHCP

Mode DHCP Configuration

Examples To distribute static routes for route `0.0.0.0/0` whose next hop is `192.16.1.1` to clients using both `opt249` and `rfc3442`, use the command:

```
awplus# configure terminal
awplus(config)# ip dhcp pool pubic
awplus(dhcp-config)# route 0.0.0.0/0 192.16.1.1 both
```

Related Commands ip dhcp pool

service dhcp-relay

Overview This command enables the DHCP Relay Agent on the device. However, on a given IP interface, no DHCP forwarding takes place until at least one DHCP server is specified to forward/relay all clients' DHCP packets to.

The **no** variant of this command disables the DHCP Relay Agent on the device for all interfaces.

Syntax

```
service dhcp-relay
no service dhcp-relay
```

Mode Global Configuration

Usage A maximum number of 400 DHCP Relay Agents (one per interface) can be configured on the device. Once this limit has been reached, any further attempts to configure DHCP Relay Agents will not be successful.

Default The DHCP-relay service is enabled by default.

Examples To enable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-relay
```

To disable the DHCP relay global function, use the commands:

```
awplus# configure terminal
awplus(config)# no service dhcp-relay
```

Related Commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

ip dhcp-relay information policy

ip dhcp-relay maxhops

ip dhcp-relay server-address

service dhcp-server

Overview This command enables the DHCP server on your device. The server then listens for DHCP requests on all IP interfaces. It will not run if there are no IP interfaces configured.

The **no** variant of this command disables the DHCP server.

Syntax

```
service dhcp-server
no service dhcp-server
```

Mode Global Configuration

Example To enable the DHCP server, use the commands:

```
awplus# configure terminal
awplus(config)# service dhcp-server
```

Related Commands

ip dhcp pool

show ip dhcp server summary

subnet-mask

show counter dhcp-client

Overview This command shows counters for the DHCP client on your device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show counter dhcp-client
```

Mode User Exec and Privileged Exec

Example To display the message counters for the DHCP client on your device, use the command:

```
awplus# show counter dhcp-client
```

Output Figure 41-1: Example output from the **show counter dhcp-client** command

```
show counter dhcp-client

DHCPDISCOVER out      ......... 10
DHCPREQUEST out       ......... 34
DHCPDECLINE out       ......... 4
DHCPRELEASE out       ......... 0
DHCPOFFER in          ......... 22
DHCPACK in            ......... 18
DHCPNAK in            ......... 0
```

Table 1: Parameters in the output of the **show counter dhcp-client** command

Parameter	Description
DHCPDISCOVER out	The number of DHCP Discover messages sent by the client.
DHCPREQUEST out	The number of DHCP Request messages sent by the client.
DHCPDECLINE out	The number of DHCP Decline messages sent by the client.
DHCPRELEASE out	The number of DHCP Release messages sent by the client.
DHCPOFFER in	The number of DHCP Offer messages received by the client.
DHCPACK in	The number of DHCP Acknowledgement messages received by the client.
DHCPNAK in	The number of DHCP Negative Acknowledgement messages received by the client.

Related Commands ip address dhcp

show counter dhcp-relay

Overview This command shows counters for the DHCP Relay Agent on your device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show counter dhcp-relay
```

Mode User Exec and Privileged Exec

Examples To display counters for the DHCP Relay Agent on your device, use the following command:

```
awplus# show counter dhcp-relay
```

Output Figure 41-2: Example output from the **show counter dhcp-relay** command

```
awplus#show counter dhcp-relay

DHCP relay counters
Requests In               ......... 4
Replies In                ......... 4
Relayed To Server         ......... 4
Relayed To Client         ......... 4
Out To Server Failed      ......... 0
Out To Client Failed      ......... 0
Invalid hlen              ......... 0
Bogus giaddr              ......... 0
Corrupt Agent Option      ......... 0
Missing Agent Option      ......... 0
Bad Circuit ID            ......... 0
Missing Circuit ID        ......... 0
Bad Remote ID             ......... 0
Missing Remote ID         ......... 0
Option Insert Failed      ......... 0
DHCPv6 Requests In        ......... 0
DHCPv6 Replies In         ......... 0
DHCPv6 Relayed to Server  ......... 0
DHCPv6 Relayed to Client  ......... 0
```

Parameter	Description
Requests In	The number of DHCP Request messages received from clients.
Replies In	The number of DHCP Reply messages received from servers.
Relayed To Server	The number of DHCP Request messages relayed to servers.

Parameter	Description
`Relayed To Client`	The number of DHCP Reply messages relayed to clients.
`Out To Server Failed`	The number of failures when attempting to send request messages to servers. This is an internal debugging counter.
`Out To Client Failed`	The number of failures when attempting to send reply messages to clients. This is an internal debugging counter.
`Invalid hlen`	The number of incoming messages dropped due to an invalid hlen field.
`Bogus giaddr`	The number of incoming DHCP Reply messages dropped due to the bogus giaddr field.
`Corrupt Agent Option`	The number of incoming DHCP Reply messages dropped due to a corrupt relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
`Missing Agent Option`	The number of incoming DHCP Reply messages dropped due to a missing relay agent information option field. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command.
`Bad Circuit ID`	The number of incoming DHCP Reply messages dropped due to a bad circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Missing Circuit ID`	The number of incoming DHCP Reply messages dropped due to a missing circuit ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command

Parameter	Description
`Bad Remote ID`	The number of incoming DHCP Reply messages dropped due to a bad remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Missing Remote ID`	The number of incoming DHCP Reply messages dropped due to a missing remote ID. Note that Agent Option counters only increment on errors occurring if the ip dhcp-relay agent-option command is configured for an interface. Messages generating the errors are only dropped if the ip dhcp-relay agent-option checking command is configured on the interface as well as the ip dhcp-relay agent-option command
`Option Insert Failed`	The number of incoming DHCP Request messages dropped due to an error adding the DHCP Relay Agent information (option-82). This counter increments when: • the DHCP Relay Agent is set to drop packets with the DHCP Relay Agent Option 82 field already filled by another DHCP Relay Agent. This policy is set with the ip dhcp-relay information policy command. • there is a packet error that stops the DHCP Relay Agent from being able to append the packet with its DHCP Relay Agent Information Option (Option 82) field.
`DHCPv6 Requests In`	The number of incoming DHCPv6 Request messages.
`DHCPv6 Replies In`	The number of incoming DHCPv6 Reply messages.
`DHCPv6 Relayed to Server`	The number of DHCPv6 messages relayed to the server.
`DHCPv6 Relayed to Client`	The number of DHCPv6 messages relayed to the client.

show counter dhcp-server

Overview This command shows counters for the DHCP server on your device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show counter dhcp-server
```

Mode User Exec and Privileged Exec

Example To display counters for the DHCP server on your device, use the command:

```
awplus# show counter dhcp-server
```

Output Figure 41-3: Example output from the **show counter dhcp-server** command

```
DHCP server counters
DHCPDISCOVER in       ......... 20
DHCPREQUEST in        ......... 12
DHCPDECLINE in        ......... 1
DHCPRELEASE in        ......... 0
DHCPINFORM in         ......... 0
DHCPOFFER out         ......... 8
DHCPACK out           ......... 4
DHCPNAK out           ......... 0
BOOTREQUEST in        ......... 0
BOOTREPLY out         ......... 0
```

Table 2: Parameters in the output of the **show counter dhcp-server** command

Parameter	Description
DHCPDISCOVER in	The number of Discover messages received by the DHCP server.
DHCPREQUEST in	The number of Request messages received by the DHCP server.
DHCPDECLINE in	The number of Decline messages received by the DHCP server.
DHCPRELEASE in	The number of Release messages received by the DHCP server.
DHCPINFORM in	The number of Inform messages received by the DHCP server.
DHCPOFFER out	The number of Offer messages sent by the DHCP server.
DHCPACK out	The number of Acknowledgement messages sent by the DHCP server.

Table 2: Parameters in the output of the **show counter dhcp-server** command

Parameter	Description
`DHCPNAK out`	The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool.
`BOOTREQUEST in`	The number of bootp messages received by the DHCP server from bootp clients.
`BOOTREPLY out`	The number of bootp messages sent by the DHCP server to bootp clients.

Related Commands

service dhcp-server

show ip dhcp binding

show ip dhcp server statistics

show ip dhcp pool

show dhcp lease

Overview This command shows details about the leases that the DHCP client has acquired from a DHCP server for interfaces on the device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare_Plus" Feature Overview and Configuration Guide.

Syntax

```
show dhcp lease [<interface>]
```

Parameter	Description
<interface>	Interface name to display DHCP lease details for.

Mode User Exec and Privileged Exec

Example To show the current lease expiry times for all interfaces, use the command:

```
awplus# show dhcp lease
```

To show the current lease for vlan1, use the command:

```
awplus# show dhcp lease vlan1
```

Output Figure 41-4: Example output from the **show dhcp lease** command

```
Interface vlan1
-----------------------------------------------------------------
IP Address:                   192.168.22.4
Expires:                      13 Mar 2007 20:10:19
Renew:                        13 Mar 2007 18:37:06
Rebind:                       13 Mar 2007 19:49:29
Server:
Options:
  subnet-mask                 255.255.255.0
  routers                     19.18.2.100,12.16.2.17
  dhcp-lease-time             3600
  dhcp-message-type           5
  domain-name-servers         192.168.100.50,19.88.200.33
  dhcp-server-identifier      192.168.22.1
  domain-name                 alliedtelesis.com

Interface vlan2
-----------------------------------------------------------------
IP Address:                   100.8.16.4
Expires:                      13 Mar 2007 20:15:39
Renew:                        13 Mar 2007 18:42:25
Rebind:                       13 Mar 2007 19:54:46
Server:
Options:
  subnet-mask                 255.255.0.0
  routers                     10.58.1.51
  dhcp-lease-time             1000
  dhcp-message-type           5
  dhcp-server-identifier      100.8.16.1
```

Related Commands ip address dhcp

show ip dhcp binding

Overview This command shows the lease bindings that the DHCP server has allocated clients.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip dhcp binding [<ip-address>|<address-pool>]
```

Parameter	Description
<ip-address>	IPv4 address of a leased IP address, in dotted decimal notation. This displays the lease information for the specified IP address.
<address-pool>	Name of an address pool. This displays the lease information for all clients within the address pool.

Mode User Exec and Privileged Exec

Examples To display all leases for every client in all address pools, use the command:

```
awplus# show ip dhcp binding
```

To display the details for the leased IP address `172.16.2.16`, use the command:

```
awplus# show ip dhcp binding 172.16.2.16
```

To display the leases from the address pool `MyPool`, use the command:

```
awplus# show ip dhcp binding MyPool
```

Output Figure 41-5: Example output from the **show ip dhcp binding** command

```
Pool 30_2_network Network 172.16.2.0/24
DHCP Client Entries
IP Address      ClientId                    Type           Expiry
------------------------------------------------------------------------------
172.16.2.100    0050.fc82.9ede              Dynamic        21 Sep 2007 19:02:58
172.16.2.101    000e.a6ae.7c14              Static         Infinite
172.16.2.102    000e.a6ae.7c4c              Static         Infinite
172.16.2.103    000e.a69a.ac91              Static         Infinite
172.16.2.104    00e0.189d.5e41              Static         Infinite
172.16.2.150    00e0.2b04.5800              Static         Infinite
172.16.2.167    4444.4400.35c3              Dynamic        21 Sep 2007 14:58:41
```

Related Commands

clear ip dhcp binding

ip dhcp pool

lease

range

service dhcp-server

show ip dhcp pool

show ip dhcp pool

Overview This command displays the configuration details and system usage of the DHCP address pools configured on the device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip dhcp pool [<address-pool>]
```

Parameter	Description
<address-pool>	Name of a specific address pool. This displays the configuration of the specified address pool only.

Mode User Exec and Privileged Exec

Example

```
awplus# show ip dhcp pool
```

Output Figure 41-6: Example output from the **show ip dhcp pool** command

```
Pool p1 :
  network: 192.168.1.0/24
  address ranges:
    addr: 192.168.1.10 to 192.168.1.18
  static host addresses:
    addr: 192.168.1.12     MAC addr: 1111.2222.3333
  lease <days:hours:minutes:seconds> <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  Probe:                        Default Values
    Status:       Enabled       [Enabled]
    Type:         ARP           [Ping]
    Packets:      2             [5]
    Timeout:      200 msecs     [200]
  Dynamic addresses:
    Total:        8
    Leased:       2
    Utilization:  25.0 %
  Static host addresses:
    Total:        1
    Leased:       1
```

Output Figure 41-7: Example output from the **show ip dhcp pool** command with IP address 192.168.1.12 assigned to a VLAN interface on the device:

```
Pool p1 :
  network: 192.168.1.0/24
  address ranges:
    addr: 192.168.1.10 to 192.168.1.18
            (interface addr 192.168.1.12 excluded)
            (static host addr 192.168.1.12 excluded)
  static host addresses:
    addr: 192.168.1.12     MAC addr: 1111.2222.3333
            (= interface addr, so excluded)
  lease <days:hours:minutes:seconds> <1:0:0:0>
  subnet mask: 255.255.255.0 (pool's network mask)
  Probe:                        Default Values
    Status:       Enabled       [Enabled]
    Type:         ARP           [Ping]
    Packets:      2             [5]
    Timeout:      200 msecs     [200]
  Dynamic addresses:
    Total:        8
    Leased:       2
    Utilization:  25.0 %
  Static host addresses:
    Total:        1
    Leased:       1
```

Table 3: Parameters in the output of the **show ip dhcp pool** command

Parameter	Description
`Pool`	Name of the pool.
`network`	Subnet and mask length of the pool.
`address ranges`	Individual IP addresses and address ranges configured for the pool. The DHCP server can offer clients an IP address from within the specified ranges only. Any of these addresses that match an interface address on the device, or a static host address configured in the pool, will be automatically excluded from the range, and a message to this effect will appear beneath the range entry.
`static host addresses`	The static host addresses configured on the pool. Each IP address is permanently assigned to the client with the matching MAC address. Any of these addresses that match an interface address on the device will be automatically excluded, and a message to this effect will appear beneath the static host entry.

Table 3: Parameters in the output of the **show ip dhcp pool** command (cont.)

Parameter	Description
`lease <days:hours:minutes>`	The lease duration for address allocated by this pool.
`domain`	The domain name sent by the pool to clients. This is the domain name that the client should use when resolving host names using DNS.
`subnet mask`	The subnet mask sent by the pool to clients.
Probe - Status	Whether lease probing is enabled or disabled.
Probe - Type	The lease probe type configured. Either ping or ARP.
Probe - Packets	The number of packets sent for each lease probe in the range 0 to 10.
Probe - Timeout	The timeout value in milliseconds to wait for a response after each probe packet is sent. In the range 50 to 5000.
`dns servers`	The DNS server addresses sent to by the pool to clients.
`default-router(s)`	The default router addresses sent by the pool to clients.
`user-defined options`	The list of user-defined options sent by the pool to clients.
`Dynamic addresses-Total`	The total number of IP addresses that have been configured in the pool for dynamic allocation to DHCP clients.
`Dynamic addresses-Leased`	The number of IP addresses in the pool that have been dynamically allocated (leased) to DHCP clients.
`Dynamic addresses - Utilization`	The percentage of IP addresses in the pool that are currently dynamically allocated to clients.
`Static host addresses-Total`	The number of static IP addresses configured in the pool for specific DHCP client hosts.
`Static host addresses - Leased`	The number of static IP addresses assigned to specific DHCP client hosts.

Related Commands

ip dhcp pool

probe enable

probe packets

probe timeout

probe type

range

service dhcp-server

subnet-mask

show ip dhcp-relay

Overview This command shows the configuration of the DHCP Relay Agent on each interface.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip dhcp-relay [interface <interface-name>]
```

Parameter	Description
<interface-name>	Name of a specific interface. This displays the DHCP configuration for the specified interface only.

Mode User Exec and Privileged Exec

Example To display the DHCP Relay Agent's configuration on the interface `vlan100`, use the command:

```
awplus# show ip dhcp-relay interface vlan100
```

Output Figure 41-8: Example output from the **show ip dhcp-relay** command

```
DHCP Relay Service is enabled

vlan100 is up, line protocol is up
Maximum hop count is 10
Insertion of Relay Agent Option is disabled
Checking of Relay Agent Option is disabled
The Remote Id string for Relay Agent Option is 0000.cd28.074c
Relay information policy is to append new relay agent
information
List of servers :   192.168.1.200
```

Related Commands

ip dhcp-relay agent-option

ip dhcp-relay agent-option checking

ip dhcp-relay information policy

ip dhcp-relay maxhops

ip dhcp-relay server-address

show ip dhcp server statistics

Overview This command shows statistics related to the DHCP server.

You can display the server counters using the show counter dhcp-server command as well as with this command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show ip dhcp server statistics
```

Mode User Exec and Privileged Exec

Example To display the server statistics, use the command:

```
awplus# show ip dhcp server statistics
```

Output Figure 41-9: Example output from the **show ip dhcp server statistics** command

```
DHCP server counters
DHCPDISCOVER in       ......... 20
DHCPREQUEST in        ......... 12
DHCPDECLINE in        ......... 1
DHCPRELEASE in        ......... 0
DHCPINFORM in         ......... 0
DHCPOFFER out         ......... 8
DHCPACK out           ......... 4
DHCPNAK out           ......... 0
BOOTREQUEST in        ......... 0
BOOTREPLY out         ......... 0
DHCPLEASEQUERY in       ....... 0
DHCPLEASEUNKNOWN out    ....... 0
DHCPLEASEACTIVE out     ....... 0
DHCPLEASEUNASSIGNED out ....... 0
```

Table 4: Parameters in the output of the **show ip dhcp server statistics** command

Parameter	Description
DHCPDISCOVER in	The number of Discover messages received by the DHCP server.
DHCPREQUEST in	The number of Request messages received by the DHCP server.
DHCPDECLINE in	The number of Decline messages received by the DHCP server.

Table 4: Parameters in the output of the **show ip dhcp server statistics** command (cont.)

Parameter	Description
DHCPRELEASE in	The number of Release messages received by the DHCP server.
DHCPINFORM in	The number of Inform messages received by the DHCP server.
DHCPOFFER out	The number of Offer messages sent by the DHCP server.
DHCPACK out	The number of Acknowledgement messages sent by the DHCP server.
DHCPNAK out	The number of Negative Acknowledgement messages sent by the DHCP server. The server sends these after receiving a request that it cannot fulfil because either there are no available IP addresses in the related address pool, or the request has come from a client that doesn't fit the network setting for an address pool.
BOOTREQUEST in	The number of bootp messages received by the DHCP server from bootp clients.
BOOTREPLY out	The number of bootp messages sent by the DHCP server to bootp clients.
DHCPLEASEQUERY in	The number of Lease Query messages received by the DHCP server from DHCP Relay Agents.
DHCPLEASEUNKNOWN out	The number of Lease Unknown messages sent by the DHCP server to DHCP Relay Agents.
DHCPLEASEACTIVE out	The number of Lease Active messages sent by the DHCP server to DHCP Relay Agents.
DHCPLEASEUNASSIGNED out	The number of Lease Unassigned messages sent by the DHCP server to DHCP Relay Agents.

Related Commands

show counter dhcp-server

service dhcp-server

show ip dhcp binding

show ip dhcp pool

show ip dhcp server summary

Overview This command shows the current configuration of the DHCP server. This includes:

- whether the DHCP server is enabled
- whether the DHCP server is configured to ignore BOOTP requests
- whether the DHCP server is configured to support DHCP lease queries
- the details of any user-defined options
- a list of the names of all DHCP address pools currently configured

This show command does not include any configuration details of the address pools. You can display these using the show ip dhcp pool command.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ip dhcp server summary
```

Mode User Exec and Privileged Exec

Example To display the current configuration of the DHCP server, use the command:

```
awplus# show ip dhcp server summary
```

Output Figure 41-10: Example output from the **show ip dhcp server summary** command

```
DHCP Server service is disabled
BOOTP ignore is disabled
DHCP leasequery support is disabled
Pool list: p2
```

Related Commands

ip dhcp leasequery enable

ip dhcp pool

service dhcp-server

subnet-mask

Overview This command sets the subnet mask option for a DHCP address pool you are configuring. Use this command to specify the client's subnet mask as defined in RFC 950. This sets the subnet details using the pre-defined option 1. Note that if you create a user-defined option 1 using the option command, then you will override any settings created with this command. If you do not specify a subnet mask using this command, then the pool's network mask (specified using the next-server command) is applied.

The **no** variant of this command removes a subnet mask option from a DHCP pool. The pool reverts to using the pool's network mask.

Syntax

```
subnet-mask <mask>
no subnet-mask
```

Parameter	Description
<mask>	Valid IPv4 subnet mask, in dotted decimal notation.

Mode DHCP Configuration

Examples To set the subnet mask option to `255.255.255.0` for DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# subnet-mask 255.255.255.0
```

To remove the subnet mask option from DHCP pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ip dhcp pool P2
awplus(dhcp-config)# no subnet-mask
```

Related Commands

default-router

dns-server

domain-name

next-server

option

service dhcp-server

show ip dhcp pool

42 DHCP for IPv6 (DHCPv6) Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure DHCPv6. For more information, see the DHCPv6 Feature Overview and Configuration Guide.

DHCPv6 is a network protocol used to configure IPv6 hosts with IPv6 addresses and IPv6 prefixes for an IPv6 network. DHCPv6 is used instead of SLAAC (Stateless Address Autoconfiguration) at sites where centralized management of IPv6 hosts is needed. IPv6 routers require automatic configuration of IPv6 addresses and IPv6 prefixes.

DHCPv6 Prefix Delegation provides automatic configuration of IPv6 addresses and IPv6 prefixes.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

NOTE: *The IPv6 addresses shown use the address space 2001:0db8::/32, defined in RFC 3849 for documentation purposes. These addresses should not be used for practical networks (other than for testing purposes) nor should they appear on any public network.*

Command List

address prefix

Overview Use this command in DHCPv6 Configuration mode to specify an address prefix for address assignment with DHCPv6 server pool configuration.

Use the **no** variant of this command to remove the address prefix from the DHCPv6 server pool.

Syntax

```
address prefix <ipv6-prefix/prefix-length> [lifetime
{<valid-time>|infinite} {<preferred-time>|infinite}]
```

```
no address prefix <ipv6-prefix/prefix-length>
```

Parameter	Description
<ipv6-prefix/prefix-length>	Specify an IPv6 prefix and prefix length, The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
`lifetime`	Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify the optional lifetime parameter with this command then you must also specify a *valid-time* and a *preferred-time* value. See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry.
<valid-time>	Specify a valid lifetime in seconds in the range <5-315360000>. The default valid lifetime is 2592000 seconds.
`infinite`	Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.
<preferred-time>	Specify a preferred lifetime in seconds in the range <5-315360000>. The default preferred lifetime is 604800 seconds.

Mode DHCPv6 Configuration

Default The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

Usage This command creates a pool of prefixes from which addresses are assigned to clients on request, and allocates a network prefix from which the DHCPv6 Server leases addresses. This command is an alternative to using a range set using the address range command.

The DHCPv6 Server selects an IPv6 address from the range available allocated by the IPv6 prefix, randomly generating the suffix of the IPv6 address, with the specified preferred and valid lifetime leases. Leased IPv6 address are found in the

DHCPv6 Server REPLY packet, which is located within the IANA (Identity Association for Non-temporary Addresses) IA address field in the **REPLY** message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

Examples To add IPv6 address prefix `2001:0db8:1::/48` for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address prefix 2001:0db8:1::/48
```

To remove a configured IPv6 address prefix for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address prefix 2001:0db8:1::/48
```

Related Commands

address range

ipv6 dhcp pool

Validation Commands

show ipv6 dhcp binding

show ipv6 dhcp pool

address range

Overview Use this command in DHCPv6 Configuration mode to specify an address range for address assignment with DHCPv6 server pool configuration.

Use the **no** variant of this command to remove an address range from the DHCPv6 server pool.

Syntax

```
address range <first-ipv6-address>
<last-ipv6-address>[lifetime {<valid-time>|infinite}
{<preferred-time>|infinite}]
```

```
no address range <first-ipv6-address> <last-ipv6-address>
```

Parameter	Description
<first-ipv6-address>	Specify the first IPv6 address of the IPv6 address range, in hexadecimal notation in the format X:X::X:X.
<last-ipv6-address>	Specify the last IPv6 address of the IPv6 address range, in hexadecimal notation in the format X:X::X:X.
lifetime	Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify this parameter then you must also specify a *valid-time* and a *preferred-time* value. See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry.
<valid-time>	Specify a valid lifetime in seconds in the range <5-31536000>. The default valid lifetime is 2592000 seconds.
infinite	Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.
<preferred-time>	Specify a preferred lifetime in seconds in the range <5-31536000>. The default preferred lifetime is 604800 seconds.

Default The default valid lifetime is 2592000 seconds and the default preferred lifetime is 604800 seconds.

Mode DHCPv6 Configuration

Usage Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

Examples To add the IPv6 address range `2001:0db8:1::1` to `2001:0db8:1fff::1` for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# address range 2001:0db8:1::1
2001:0db8:1fff::1
```

To remove a configured IPv6 address range for DHCPv6 server pool configuration, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# no address range
```

Related Commands
address prefix
ipv6 dhcp pool

Validation Commands
show ipv6 dhcp binding
show ipv6 dhcp pool

clear counter ipv6 dhcp-client

Overview Use this command in Privileged Exec mode to clear DHCPv6 client counters.

Syntax

```
clear counter ipv6 dhcp-client
```

Mode Privileged Exec

Example To clear DHCPv6 client counters, use the following command:

```
awplus# clear counter ipv6 dhcp-client
```

Related Commands show counter ipv6 dhcp-client

clear counter ipv6 dhcp-server

Overview Use this command in Privileged Exec mode to clear DHCPv6 server counters.

Syntax

```
clear counter ipv6 dhcp-server
```

Mode Privileged Exec

Example To clear DHCPv6 server counters, use the following command:

```
awplus# clear counter ipv6 dhcp-server
```

Related Commands show counter ipv6 dhcp-server

clear ipv6 dhcp binding

Overview Use this command in Privileged Exec mode to clear either a specific lease binding or the lease bindings as specified by the command parameters. The command will only take effect on dynamically allocated bindings, not statically configured bindings. This command clears binding entries on the DHCPv6 server binding table.

Syntax `clear ipv6 dhcp binding {ipv6 <prefix>|duid <DUID>|all|pool <name>}`

Parameter	Description
`ipv6 <prefix>`	Optional. Specify the IPv6 prefix of the DHCPv6 client, in hexadecimal notation in the format `X:X::X:X`.
`duid <DUID>`	Specify the DUID (DHCPv6 unique ID) of the DHCPv6 client.
`all`	All DHCPv6 bindings.
`pool <name>`	Description used to identify DHCPv6 server address pool. Valid characters are any printable character. If the name contains spaces then you must enclose these in "quotation marks".

Mode Privileged Exec

Usage A specific binding may be deleted by **ipv6** address or **duid** address, or several bindings may be deleted at once using **all** or **pool**.

Note that if you specify to clear the **ipv6** or **duid** address of what is actually a static DHCPv6 binding, an error message is displayed. If **all** or **pool** are specified and one or more static DHCPv6 bindings exist within those addresses, any dynamic entries within those addresses are cleared but any static entries are not cleared.

The clear ipv6 dhcp binding command is used as a server function. A binding table entry on the DHCPv6 server is automatically:

- Created whenever a prefix is delegated to a client from the configuration pool.
- Updated when the client renews, rebinds, or confirms the prefix delegation.
- Deleted when the client releases all the prefixes in the binding, all prefix lifetimes have expired, or when a user runs the clear ipv6 dhcp binding command.

If the **clear ipv6 dhcp binding** command is used with the optional IPv6 address parameter, only the binding for the specified client is deleted. If the **clear ipv6 dhcp binding** command is used without the optional IPv6 address parameter, then all automatic client bindings are deleted from the DHCPv6 bindings table.

Example To clear all dynamic DHCPv6 server binding entries, use the command:

```
awplus# clear ipv6 dhcp binding all
```

Output Figure 42-1: Example output from the **clear ipv6 dhcp binding all** command

```
awplus#clear ipv6 dhcp binding all
% Deleted 1 entries
```

Related Commands show ipv6 dhcp binding

clear ipv6 dhcp client

Overview Use this command in Privileged Exec mode to restart a DHCPv6 client on an interface.

Syntax

```
clear ipv6 dhcp client <interface>
```

Parameter	Description
<interface>	Specify the interface name to restart a DHCPv6 client on.

Mode Privileged Exec

Example To restart a DHCPv6 client on interface vlan1, use the following command:

```
awplus# clear ipv6 dhcp client vlan1
```

Related Commands show ipv6 dhcp binding

dns-server (DHCPv6)

Overview Use this command to add a Domain Name System (DNS) server to the DHCPv6 address pool you are configuring. You can use this command multiple times to create a list of DNS name servers available to the client. This sets the DNS server details using the pre-defined option 6. Note that if you add a user-defined option 6 using the option (DHCPv6) command, then you will override any settings created with this command.

Use the **no** variant of this command to remove either the specified DNS server or all DNS servers from the DHCPv6 pool.

Syntax

```
dns-server <ipv6-address>
no dns-server [<ipv6-address>]
```

Parameter	Description
<ipv6-address>	Specify an IPv6 address of the DNS server, in hexadecimal notation in the format X:X::X:X. This parameter is required when adding a DNS server to the DHCPv6 address pool. All DNS servers are removed from the DHCPv6 pool if you enter the no dns-server command without this parameter.

Mode DHCPv6 Configuration

Examples To add the DNS server with the assigned IPv6 address 2001:0db8:3000:3000::32 to the DHCPv6 server pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# dns-server 2001:0db8:3000:3000::32
```

To remove the DNS server with the assigned IPv6 address 2001:0db8:3000:3000::32 from the DHCPv6 server pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server 2001:0db8:3000:3000::32
```

To remove all DNS servers from the DHCPv6 server pool named P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no dns-server
```

Related Commands

ipv6 dhcp pool

option (DHCPv6)

show ipv6 dhcp pool

domain-name (DHCPv6)

Overview Use this command in DHCPv6 Configuration mode to add a domain name to the DHCPv6 server address pool you are configuring.

Use the **no** variant of this command to remove a domain name from the address pool.

Syntax

```
domain-name <domain-name>
no domain-name
```

Parameter	Description
<domain-name>	Specify the domain name you wish to assign the DHCPv6 server address pool. Valid characters are printable characters. If the name contains spaces then you must enclose it in "quotation marks".

Mode DHCPv6 Configuration

Usage This command specifies the domain name that a client should use when resolving host names using the Domain Name System, and sets the domain name details using the pre- defined option 15. Note that if you add a user-defined option 15 using the option (DHCPv6) command, then you will override any settings created with this command.

Examples To add the domain name `Engineering` to DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# domain-name Engineering
```

To remove the domain name `Engineering` from DHCPv6 server pool `P2`, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(dhcpv6-config)# no domain-name Engineering
```

Related Commands

dns-server (DHCPv6)

option (DHCPv6)

show ipv6 dhcp pool

ip dhcp-relay agent-option subscriber-id-auto-mac

Overview This command causes the relay agent to insert the requesting clients' MAC address into a subscriber ID field in the relay header. A suitably-configured server can then use this subscriber ID option to assign the same IPv6 address to that requesting client every time it requires an address.

Use the no form of this command to disable this feature.

Syntax

```
ip dhcp-relay agent-option subscriber-id-auto-mac
no ip dhcp-relay agent-option subscriber-id-auto-mac
```

Default Disabled

Usage By default, DHCPv6 uses a DUID-LLT client identifier instead of a MAC address. This is generated by the operating system when DHCP first starts. If the OS is reinstalled the DUID-LLT can change, and any multiple operating systems on the machine will all have different DUIDs.

Configuring the subscriber-id-auto-mac option causes the relay agent to insert the requesting client's MAC address into a subscriber ID field in the relay header. A suitably-configured server can then use this subscriber ID to assign the same IPv6 address to that requesting client every time it connects.

The client must be in the same L2 network as the relay. If there are multiple relays between the client and the server, only the first relay will add a subscriber ID option.

Example To enable this feature on VLAN1, use the following commands:

```
awplus(config)#int vlan1
awplus(config-if)#ip dhcp-relay agent-option
subscriber-id-auto-mac
```

For an example of how to configure a relay agent and server, see the document "How to use DHCPv6 to assign specific IPv6 addresses to specific devices", available from www.alliedtelesis.com.

ipv6 address (DHCPv6 PD)

Overview Use this command in Interface Configuration mode for a VLAN interface to append an IPv6 address suffix to the IPv6 prefix provided by a DHCPv6 Prefix Delegation (PD) server.

Use the **no** variant of this command to remove the IPv6 address assigned and disable IPv6. Note that if no global addresses are left after removing the IPv6 address then IPv6 is disabled.

Syntax

```
ipv6 address [<ipv6-prefix-name>] <ipv6-addr/prefix-length>
[eui64]
```

```
no ipv6 address [<ipv6-prefix-name>] <ipv6-addr/prefix-length>
[eui64]
```

Parameter	Description
<ipv6-prefix-name>	The IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.
<ipv6-addr/prefix-length>	Specifies the IPv6 address to be set, for example ::1/64. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
[eui64]	EUI-64 is a method of automatically deriving the lower 64 bits of an IPv6 address, based on the switch's MAC address.

Mode Interface Configuration for a VLAN interface.

Mode Interface Configuration for a VLAN interface or Interface Configuration for a PPP interface.

Usage When specifying the **eui64** parameter, the interface identifier of the IPv6 address is derived from the MAC address of the device.

For more information about EUI64, see the IPv6 Feature Overview and Configuration Guide.

Examples To configure a PD prefix named prefix1 on interface vlan1 and then add an IPv6 address, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1::1/64
```

In this example, the prefix will be assigned from the pool on the PD client. The host portion or suffix will be ::1 for the last 64 bits.

To configure a PD prefix named prefix1 on interface vlan1 and then add an IPv6 address using EUI-64 identifiers, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan1
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 address prefix1/64 eui64
```

In this example, the prefix will be assigned from the pool on the PD client. The host portion or suffix is created from the EUI-64 identifier of the interface for the last 64 bits.

To assign the IPv6 address 2001:0db8::a2/48 to the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::a2/48
```

To remove the IPv6 address 2001:0db8::a2/48 from the VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::a2/48
```

To assign the IPv6 address to the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-fr-subif)# ipv6 address 2001:0db8::a2/64
```

To remove the IPv6 address 2001:0db8::a2/64 from the PPP interface `ppp0`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address 2001:0db8::a2/64
```

To assign the **eui64** derived address in the prefix `2001:db8::/64` to VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 address 2001:0db8::/64 eui64
```

To remove the **eui64** derived address in the prefix `2001:db8::/32` from VLAN interface `vlan2`, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 address 2001:0db8::/64 eui64
```

Validation Commands

show running-config

show ipv6 dhcp binding

show ipv6 interface brief

show ipv6 route

Related Commands

ipv6 dhcp client pd

ipv6 dhcp pool

ipv6 local pool

ipv6 nd prefix (DHCPv6)

prefix-delegation pool

ipv6 address dhcp

Overview Use this command in Interface Configuration mode to activate the DHCPv6 client on the interface that you are configuring. This allows the interface to use the DHCPv6 client to obtain its IPv6 configuration details from a DHCPv6 server on its connected network.

Use the **no** variant of this command to stop the interface from obtaining IPv6 configuration details from a DHCPv6 server.

The DHCPv6 client supports the following IP configuration options:

- Option 1 - the subnet mask for your device.
- Option 3 - a list of default routers.
- Option 6 - a list of DNS servers. This list appends the DNS servers set on your device with the dns-server (DHCPv6) command.
- Option 15 - a domain name used to resolve host names. This option replaces any domain name that you have set with the domain-name (DHCPv6) command.
- Option 51 - lease expiration time.

Syntax

```
ipv6 address dhcp
no ipv6 address dhcp
```

Mode Interface Configuration for a VLAN interface or a local loopback interface.

Examples To set the interface `vlan10` to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config)# ipv6 enable
awplus(config-if)# ipv6 address dhcp
```

To stop the interface `vlan10` from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface vlan10
awplus(config-if)# no ipv6 address dhcp
```

To set the PPP interface `ppp0` to use DHCPv6 to obtain an IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# ipv6 address dhcp
```

To stop to the PPP interface `ppp0` from using DHCPv6 to obtain its IPv6 address, use the commands:

```
awplus# configure terminal
awplus(config)# interface ppp0
awplus(config-if)# no ipv6 address dhcp
```

Related Commands ipv6 address

Validation Commands show running-config

ipv6 dhcp client pd

Overview Use this command in Interface Configuration mode to enable the DHCPv6 client process and enable requests for prefix delegation through the interface that you are configuring.

Use the **no** variant of this command to disable requests for prefix delegation. This is the default setting.

For further information about DHCPv6 Prefix Delegation, which is used to automate the process of assigning prefixes, see the DHCPv6 Feature Overview and Configuration Guide.

Syntax

```
ipv6 dhcp client pd <prefix-name>
no ipv6 dhcp client pd
```

Parameter	Description
<prefix-name>	Specify an IPv6 general prefix name. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".

Mode Interface Configuration

Default Prefix delegation is disabled by default on an interface.

Usage Entering the **ipv6 dhcp client pd** command starts the DHCPv6 client process if not already running, and enables requests for prefix delegation through the interface on which the command is configured.

When prefix delegation is enabled and a prefix is acquired, the prefix is stored in the IPv6 prefix pool with an internal name defined by the required *<prefix-name>* placeholder parameter. The ipv6 address command can then refer to the prefixes stored in the IPv6 prefix pool.

Examples To enable prefix delegation with the prefix name prefix-name on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd my-prefix-name
```

To disable prefix delegation on the VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 dhcp client pd
```

Related Commands

clear ipv6 dhcp client

ipv6 address (DHCPv6 PD)

ipv6 nd prefix (DHCPv6)

show ipv6 dhcp binding

ipv6 dhcp option

Overview Use this command in Global Configuration mode to create a user-defined DHCPv6 option. You can then use this option when configuring a DHCPv6 server address pool, by using the option (DHCPv6) command.

Options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

Use the **no** variant of this command to remove either the specified user-defined option. This also removes user-defined options from the associated DHCPv6 server address pools.

Syntax

```
ipv6 dhcp option <1-254> [name <option-name>] [<option-type>]
no ipv6 dhcp option <1-254>|<option-name>
```

Parameter	Description	
<1-254>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.	
<option-name>	Option name used to identify the option. You cannot use a number as the option name. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”. Default: no default	
<option-type>	The option value. You must specify a value that is appropriate to the option type:	
	`asci`	An ASCII text string
	`hex`	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	`ipv6`	An IPv6 address or prefix that has hexadecimal notation in the format `HHHH:HHHH::HHHH:HHHH`. To create a list of IPv6 addresses, you must add each IPv6 address individually by using the option command multiple times.
	`integer`	A number from 0 to 4294967295.
	`flag`	A value that either sets (to 1) or unsets (to 0) a flag: **true**, **on**, or **enabled** will set the flag. **f alse**, **off** or **disabled** will unset the flag.

Mode Global Configuration

Examples

To define a user-defined ASCII string option as option 66, without a name, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 66 ascii
```

To define a user-defined hexadecimal string option as option 46, with the name “tcpip- node-type”, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 46 name tcpip-node-type hex
```

To define a user-defined IP address option as option 175, with the name `special-address`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 175 name special-address ip
```

To remove the specific user-defined option with the option number `12`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option 12
```

To remove the specific user-defined option with the option name `perform-router-discovery`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp option perform-router-discovery
```

Related Commands

dns-server (DHCPv6)

domain-name (DHCPv6)

option (DHCPv6)

show ipv6 dhcp

ipv6 dhcp pool

Overview Use this command in Global Configuration mode to enter the DHCPv6 Configuration mode for the DHCPv6 server pool name as specified in the required command parameter. If the name specified is not associated with an existing pool, the device will create a new pool with this name, then enter the configuration mode for the new pool.

Once you have entered the DHCPv6 configuration mode, all commands executed before the next **exit** command will apply to this pool.

You can create multiple DHCPv6 server pools on devices with multiple interfaces. This allows the device to act as a DHCPv6 server on multiple interfaces to distribute different information to clients on the different networks.

Use the **no** variant of this command to delete the specific DHCPv6 pool.

Syntax

```
ipv6 dhcp pool <DHCPv6-poolname>
no ipv6 dhcp pool <DHCPv6-poolname>
```

Parameter	Description
<DHCPv6-poolname>	Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”.

Mode Global Configuration

Usage All DHCPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

Examples To create the DHCPv6 pool named `P2` and enter DHCPv6 configuration mode, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)#
```

To delete the DHCPv6 pool named `P2`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 dhcp pool P2
```

Related Commands

ipv6 local pool

option (DHCPv6)

prefix-delegation pool

show ipv6 dhcp binding

show ipv6 dhcp pool

ipv6 dhcp server

Overview Use this command in Interface Configuration mode to enable DHCPv6 server for the current IPv6 configured interface to use the specified DHCPv6 server pool name.

The DHCPv6 server service listens for DHCPv6 requests on the IPv6 configured interface. The DHCPv6 server service does not run on interfaces without IPv6 configured on them.

Use the **no** variant of this command to disable the DHCPv6 server.

Syntax

```
ipv6 dhcp-server [<DHCPv6-poolname>]
no ipv6 dhcp-server
```

Parameter	Description
<DHCPv6-poolname>	Specify a named DHCPv6 server pool as defined with the ipv6 dhcp pool command. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".

Mode Interface Configuration

Usage The **ipv6 dhcp server** command enables the DHCPv6 service on a specified interface using the pool for prefix delegation and configuration through the specified interface.

Note that DHCPv6 client, DHCPv6 server and DHCPv6 relay are mutually exclusive on an interface. When one of the DHCPv6 functions is enabled on an interface then another DHCPv6 function cannot be enabled on the same interface.

Examples To enable the DHCPv6 server service and use the DHCPv6 pool named P2 on VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 dhcp server P2
```

To disable the DHCPv6 server on VLAN interface vlan2, use the following commands:

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# no ipv6 dhcp server
```

Related Commands

ipv6 dhcp pool

show ipv6 dhcp binding

show ipv6 dhcp pool

ipv6 local pool

Overview Use this command in Global Configuration mode to configure a local DHCPv6 server prefix delegation pool specifying a poolname and a prefix/prefix length. You can optionally exclude the locally assigned prefix from the pool with the **exclude-local-prefix** keyword.

Use the **no** variant of this command to remove a local DHCPv6 server prefix delegation pool specifying the poolname.

Syntax

```
ipv6 local pool <DHCPv6-poolname> <delegated-prefix-name>
<ipv6-prefix/prefix-length> <assigned-length>
[exclude-local-prefix]

no ipv6 local pool
```

Parameter	Description
<DHCPv6-poolname>	Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in “quotation marks”.
<delegated-prefix-name>	Description used to identify the delegated prefix name from the parent PD (Prefix Delegation) server. If the name contains spaces then you must enclose it in “quotation marks”.
<ipv6-prefix/prefix-length>	Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.
<assigned-length>	Specify an IPv6 prefix length assigned to the user from the pool in the range <1-128>. Note that the value of the *assigned-length* parameter entered cannot be less than or equal to the *prefix-length* parameter value entered. An assigned length must be longer than a prefix length.
exclude-local-prefix	Optional. Specify this keyword to exclude the locally assigned prefix from the pool.

Default No DHCPv6 server prefix delegation pool is configured by default.

Mode Global Configuration

Usage All IPv6 prefix pool names must be unique. IPv6 prefix pools have a similar function to IPv4 address pools. Contrary to IPv4, a block of IPv6 addresses (an IPv6 address prefix) are assigned and not single IPv6 addresses. IPv6 prefix pools are not allowed to overlap.

Once a pool is configured, it cannot be changed. To change the configuration, you must remove then recreate a IPv6 prefix pool. All IPv6 prefixes already allocated are also freed.

Examples To create a local DHCPv6 local pool named P2 with the IPv6 prefix and prefix length 2001:0db8::/32 with an assigned length of 64, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 local pool P2 2001:0db8::/32 64
```

To remove a configured DHCPv6 local pool, use the following commands:

```
awplus# configure terminal
awplus(config)# no ipv6 local pool
```

Related Commands

ipv6 dhcp pool

show ipv6 dhcp pool

ipv6 nd prefix (DHCPv6)

Overview Use this command to specify IPv6 RA (Router Advertisement) prefix information generated from the DHCPv6 server for DHCPv6 prefix-delegation for a VLAN.

Use the **no** variant of this command to remove IPv6 RA prefix information from the DHCPv6 Server for DHCPv6 Prefix-Delegation for the interface. Use the **all** parameter with the **no** variant of this command to remove all prefix names and all prefixes for an interface.

Syntax

```
ipv6 nd prefix <ipv6-prefix-name>
<ipv6-prefix/length>{<valid-lifetime>|infinite}
{<preferred-lifetime>|infinite} {off-link|no-autoconfig}
```

```
no ipv6 nd prefix {<ipv6-prefix-name>|<ipv6-prefix/length>|all}
```

Parameter	Description
<ipv6-prefix-name>	The IPv6 prefix name advertised on the router advertisement message sent from the device. The IPv6 prefix name is delegated from the DHCPv6 Server configured for DHCPv6 Prefix-Delegation.
<ipv6-prefix/length>	The IPv6 prefix and prefix length advertised on the router advertisement message sent from the device. The IPv6 address prefix uses the format X:X::/prefix-length. The prefix-length is usually set between 0 and 64. .
<valid-lifetime>	The the period during which the specified IPv6 address prefix is valid. This can be set to a value between 5 and 315360000 seconds. Note that this period should be set to a value greater than that set for the prefix preferred-lifetime. See the Usage notes after this parameter table for a description of valid lifetime and how it determines invalid IPv6 addresses upon expiry.
`infinite`	Specifying this keyword instead of entering a value for the <*valid-lifetime*> parameter applies an infinite valid lifetime.
<preferred-lifetime>	Specifies the IPv6 prefix preferred lifetime. This is the period during which the IPv6 address prefix is considered current. Set this to a value between 0 and 315360000 seconds. Note that this period should be set to a value less than that set for the prefix valid-lifetime. See the Usage notes after this parameter table for a description of preferred lifetime and how it determines deprecated IPv6 addresses upon expiry.
`infinite`	Specifying this keyword instead of entering a value for the <*preferred-lifetime*> parameter applies an infinite valid lifetime.
`off-link`	Specify the IPv6 prefix off-link flag.
`no-autoconfig`	Specify the IPv6 prefix no autoconfiguration flag. Setting this flag indicates that the prefix is not to be used for autoconfiguration.
`all`	Specify all prefix names and all prefixes are removed when used with the no variant of this command.

Mode Interface Configuration for a VLAN interface.

Mode Interface Configuration for a VLAN interface or Interface Configuration for a PPP interface.

Usage This command specifies the IPv6 prefix flags that are advertised by the router advertisement message.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

Examples The following example configures the device to issue RAs (Router Advertisements) on the VLAN interface `vlan4`, and advertises the DHCPv6 prefix name prefix1 and the IPv6 address prefix of `2001:0db8::/32`.

```
awplus# configure terminal
awplus(config)# interface vlan2
awplus(config-if)# ipv6 enable
awplus(config-if)# ipv6 dhcp client pd prefix1
awplus(config-if)# ipv6 nd prefix prefix1 2001:0db8::/32
```

The following example resets router advertisements on the VLAN interface `vlan4`, so the address prefix of `2001:0db8::/32`is not advertised from the device.

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix 2001:0db8::/32
```

The following example removes all prefix names and prefixes from VLAN interface vlan4:

```
awplus# configure terminal
awplus(config)# interface vlan4
awplus(config-if)# no ipv6 nd prefix all
```

Related Commands

ipv6 address (DHCPv6 PD)

ipv6 dhcp client pd

ipv6 dhcp pool

ipv6 local pool

prefix-delegation pool

show ipv6 dhcp binding

link-address

Overview Use this command in DHCPv6 Configuration mode to specify a link-address prefix within a DHCPv6 Server pool.

Note that you can only configure one link address per DHCPv6 pool. Configuring another link address in the same DHCPv6 pool overwrites the previously configured link address.

Use the **no** variant of this command to remove the link-address prefix from the DHCPv6 Server pool.

Syntax

```
link-address <ipv6-prefix/prefix-length>
no link-address
```

Parameter	Description
<ipv6-prefix/prefix-length>	Specify an IPv6 prefix and prefix length. The prefix length indicates the length of the IPv6 prefix assigned to the pool. The IPv6 address uses the format X:X::X:X/Prefix-Length. The prefix-length is usually set between 0 and 64.

Default No DHCPv6 Server pool configuration link address prefix is configured by default.

Mode DHCPv6 Configuration

Usage Link addresses are configured in DHCPv6 Server address pools when there are remote clients that communicate via intermediate relay(s).

RELAY-FORW and RELAY-REPL relay packets contain the requesting link address source.

This command is used to match incoming requests from PD (Prefix Delegation) clients (received via an intermediate relay) to a configured delegation pool.

When an address on the incoming interface of the DHCPv6 server or a link address set in the incoming delegation request packet from the prefix delegation client matches the link-address prefix configured in the delegation pool, the DHCPv6 server is able to match and use the appropriate delegation pool for relayed delegation request messages.

If there is no match between incoming delegation request packets from the prefix delegation client and the link-address prefix configured in the delegation pool, the DHCPv6 Server does not delegate an IPv6 prefix to the requesting device.

The link address should be set to the network prefix where the prefix delegation client resides. The prefix delegation server will also need a forwarding path (IPv6 route) back to the network prefix where the prefix delegation client resides.

For more information, see the DHCPv6 Feature Overview and Configuration Guide.

Examples

To configure the IPv6 prefix and prefix length 2001:0db8:1::/48 as the link address for pool P2, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# address prefix 2001:0db8:2::/48
awplus(config-dhcp6)# link-address 2001:0db8:1::/48
```

To remove the link address, use the commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no link-address
```

Related Commands

ipv6 dhcp pool

show ipv6 dhcp pool

option (DHCPv6)

Overview Use this command in DHCPv6 Configuration mode to add a user-defined option to the DHCPv6 prefix pool you are configuring. For the **hex**, **integer**, and **flag** option types, if the option already exists, the new option overwrites the existing option's value.

Use the **no** variant of this command to remove the specified user-defined option from the DHCPv6 server pool, or to remove all user-defined options from the DHCPv6 server pool.

Syntax

```
option [<1-254>|<option-name>] <option-value>
no option [<1-254>|<option-value>]
```

Parameter	Description	
<1-254>	The option number of the option. Options with the same number as one of the standard options overrides the standard option definition.	
<option-name>	Option name associated with the option.	
<option-value>	The option value. You must specify a value that is appropriate to the option type:	
	`hex`	A hexadecimal string. Valid characters are the numbers 0–9 and letters a–f. Embedded spaces are not valid. The string must be an even number of characters, from 2 and 256 characters long.
	`ipv6`	An IPv6 prefix that has the hexadecimal `X:X::X:X` notation. To create a list of IPv6 prefixes, you must add each IPv6 prefix individually using this command multiple times.
	`integer`	A number from 0 to 4294967295.
	`flag`	A value of either true, on, or enabled to set the flag, or false, off or disabled to unset the flag.

Mode DHCPv6 Configuration

Usage You must define a DHCPv6 option using the ipv6 dhcp option command before using the option (DHCPv6) command.

Note that options with an **ipv6** type can hold a list of IPv6 prefix (i.e. entries that have the`X:X::X:X` address format), so if the option already exists in the pool, then the new IP address is added to the list of existing IPv6 prefixes. Also note options with the same number as one of the pre-defined options override the standard option definition. The pre-defined options use the option numbers 1, 3, 6, 15, and 51.

Examples

To add the IPv6 type option named `sntp-server-addr` to the pool `P2` and give the option the value `ipv6`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp option 22 name sntp_server_addr ipv6
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option sntp_server_addr ipv6
```

To add the ASCII-type option named `tftp-server-name` to the pool `P2` and give the option the value `server1`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tftp-server-name server1
```

To add the hex-type option named `tcpip-node-type` to the pool `P2`and give the option the value `08af`, use the following commands:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# option tcpip-node-type 08af
```

To add multiple IP addresses for the ip-type option `175`, use the following commands:

```
awplus(config-dhcp6)# option 175 2001:0db8:3001::/64
awplus(config-dhcp6)# option 175 2001:0db8:3002::/64
awplus(config-dhcp6)# option 175 2001:0db8:3003::/64
```

To add the option `179` to a pool, and give the option the value `123456`, use the following command:

```
awplus(config-dhcp6)# option 179 123456
```

To add a user-defined flag option with the name `perform-router-discovery`, use the following command:

```
awplus(config-dhcp6)# option perform-router-discovery yes
```

To clear all user-defined options from a DHCP address pool, use the following command:

```
awplus(config-dhcp6)# no option
```

To clear a user-defined option, named `tftp-server-name`, use the following command:

```
awplus(config-dhcp6)# no option tftp-server-name
```

Related Commands

dns-server (DHCPv6)

ipv6 dhcp option

ipv6 dhcp pool

show ipv6 dhcp pool

prefix-delegation pool

Overview Use this command in DHCPv6 Configuration mode to add a DHCPv6 server prefix-delegation pool entry to the current DHCPv6 pool configuration. You must define a DHCPv6 server prefix-delegation pool using the ipv6 dhcp pool command before using this command.

Use the **no** variant of this command to remove a DHCPv6 server prefix-delegation pool from the current DHCPv6 pool configuration.

Syntax
```
prefix-delegation pool <DHCPv6-poolname> [lifetime
{<valid-time>|infinite} {<preferred-time>|infinite}]
no prefix-delegation pool <DHCPv6-poolname>
```

Parameter	Description
<DHCPv6-poolname>	Description used to identify this DHCPv6 server pool. Valid characters are any printable character. If the name contains spaces then you must enclose it in "quotation marks".
lifetime	Optional. Specify a time period for the hosts to remember router advertisements (RAs). If you specify this parameter then you must also specify a *valid-time* and a *preferred-time* value. See the Usage notes below this parameter table for a description of preferred and valid lifetimes and how these determine deprecated or invalid IPv6 addresses upon expiry.
<valid-time>	Specify a valid lifetime in seconds in the range <5-315360000>.
infinite	Specify an infinite valid lifetime or an infinite preferred lifetime, or both, when using this keyword.
<preferred-time>	Specify a valid lifetime in seconds in the range <5-315360000>.

Default No IPv6 local prefix pool is specified by default.

Mode DHCPv6 Configuration

Usage The DHCPv6 server assigns prefixes dynamically from an IPv6 local prefix pool, which is configured using the ipv6 local pool command and is associated with a DHCPv6 configuration pool using this command. When the server receives a prefix request from a client, it attempts to obtain unassigned prefixes from the pool. After the client releases the previously assigned prefixes, the server returns the prefixes to the pool for reassignment.

Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires.

Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source

address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.

An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

Example This example adds DHCPv6 Prefix Delegation pool pd_pool1 to DHCPv6 pool pool1:

```
awplus# configure terminal
awplus(config)# ipv6 local pool pd_pool1 2001:0db8::/48 56
awplus(config)# ipv6 dhcp pool pool1
awplus(config-dhcp6)# prefix-delegation pool pd_pool1
```

Related Commands

ipv6 dhcp pool

ipv6 local pool

show ipv6 dhcp pool

show counter ipv6 dhcp-client

Overview Use this command in User Exec or Privilege Exec mode to show DHCPv6 client counter information. See show counter ipv6 dhcp-server for DHCPv6 server information.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show counter ipv6 dhcp-client
```

Mode User Exec and Privileged Exec

Example To display the DHCPv6 client counter information, use the command:

```
awplus# show counter ipv6 dhcp-client
```

Output Figure 42-2: Example output from the **show counter ipv6 dhcp-client** command

```
awplus#show counter ipv6 dhcp-client
SOLICIT out              ......... 20
ADVERTISE in             ......... 12
REQUEST out              ......... 1
CONFIRM out              ......... 0
RENEW out                ......... 0
REBIND out               ......... 0
REPLY in                 ......... 0
RELEASE out              ......... 0
DECLINE out              ......... 0
INFORMATION-REQUEST out  ......... 0
```

Table 1: Parameters in the output of the **show counter ipv6 dhcp-client** command

Parameter	Description
SOLICIT out	Displays the count of SOLICIT messages sent by the DHCPv6 client.
ADVERTISE in	Displays the count of ADVERTISE messages received by the DHCPv6 client.
REQUEST out	Displays the count of REQUEST messages sent by the DHCPv6 client.
CONFIRM out	Displays the count of CONFIRM messages sent by the DHCPv6 client.
RENEW out	Displays the count of RENEW messages sent by the DHCPv6 client.

Table 1: Parameters in the output of the **show counter ipv6 dhcp-client** command (cont.)

Parameter	Description
`REBIND out`	Displays the count of REBIND messages sent by the DHCPv6 client.
`REPLY in`	Displays the count of REPLY messages received by the DHCPv6 client.
`RELEASE out`	Displays the count of RELEASE messages sent by the DHCPv6 client.
`DECLINE out`	Displays the count of DECLINE messages sent by the DHCPv6 client.
`INFORMATION-REQUEST out`	Displays the count of INFORMATION-REQUEST messages sent by the DHCPv6 client.

Related Commands show counter ipv6 dhcp-server

show counter ipv6 dhcp-server

Overview Use this command in User Exec or Privileged Exec mode to show DHCPv6 server counter information. See show counter ipv6 dhcp-client for DHCPv6 client information.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax
```
show counter ipv6 dhcp-server
```

Mode User Exec and Privileged Exec

Example To display the DHCPv6 server counter information, use the command:

```
awplus# show counter ipv6 dhcp-server
```

Output Figure 42-3: Example output from the **show counter ipv6 dhcp-server** command

```
awplus#show counter ipv6 dhcp-server
SOLICIT in              ......... 20
ADVERTISE out           ......... 12
REQUEST in              ......... 1
CONFIRM in              ......... 0
RENEW in                ......... 0
REBIND in               ......... 0
REPLY out               ......... 0
RELEASE in              ......... 0
DECLINE in              ......... 0
INFORMATION-REQUEST in  ......... 0
```

Table 2: Parameters in the output of the **show counter ipv6 dhcp-server** command

Parameter	Description
SOLICIT in	Displays the count of SOLICIT messages received by the DHCPv6 server.
ADVERTISE out	Displays the count of ADVERTISE messages sent by the DHCPv6 server.
REQUEST in	Displays the count of REQUEST messages received by the DHCPv6 server.
CONFIRM in	Displays the count of CONFIRM messages received by the DHCPv6 server.
RENEW in	Displays the count of RENEW messages received by the DHCPv6 server.

Table 2: Parameters in the output of the **show counter ipv6 dhcp-server** command (cont.)

Parameter	Description
`REBIND in`	Displays the count of REBIND messages received by the DHCPv6 server.
`REPLY out`	Displays the count of REPLY messages sent by the DHCPv6 server.
`RELEASE in`	Displays the count of RELEASE messages received by the DHCPv6 server.
`DECLINE in`	Displays the count of DECLINE messages received by the DHCPv6 server.
`INFORMATION-REQUEST in`	Displays the count of INFORMATION-REQUEST messages received by the DHCPv6 server

Related Commands show counter ipv6 dhcp-client

show ipv6 dhcp

Overview Use this command in User Exec or Privileged Exec mode to show the DHCPv6 unique identifier (DUID) configured on your device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 dhcp
```

Mode User Exec and Privileged Exec

Usage The DUID is based on the link-layer address for both DHCPv6 client and DHCPv6 server identifiers. The device uses the MAC address from the lowest interface number for the DUID.

The DUID is used by a DHCPv6 client to obtain an IPv6 address from a DHCPv6 server. A DHCPv6 server compares the DUID with its database of DUIDs and sends configuration data for an IPv6 address plus the preferred and valid lease time values to a DHCPv6 client.

Example To display the DUID configured on your device, use the command:

```
awplus# show ipv6 dhcp
```

Output Figure 42-4: Example output from the **show ipv6 dhcp** command

```
awplus#show ipv6 dhcp
DHCPv6 Server DUID: 0001000117ab6876001577f7ba23
```

Related Commands ipv6 address dhcp

show ipv6 dhcp binding

Overview Use this command in User Exec or Privileged Exec mode to show the IPv6 address entries that the DHCPv6 server leases to DHCPv6 clients. Note that applying this command with the optional *summary* keyword parameter displays the number of addresses per pool, but not the address or prefix entries per pool.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 dhcp binding [summary]
```

Parameter	Description
`summary`	Optional. Specify the **summary** keyword to display summarized information for DHCPv6 server leases to client nodes, displaying the number of address entries per pool, not the addresses or prefixes.

Mode User Exec and Privileged Exec

Example 1 To display the total DHCPv6 leasing address entries for all pools, use the command:

```
awplus# show ipv6 dhcp binding summary
```

Output Figure 42-5: Example output from the **show ipv6 dhcp binding summary** command

```
awplus# show ipv6 dhcp binding summary
Pool Name                  Number of Leased Addresses
-----------------------------------------------------
ia-na1                     3
ia-pd1                     5

Total in all Pools:        8
```

Table 3: Parameters in the output of the **show ipv6 dhcp binding summary** command

Parameter	Description
`Pool Name`	Displays a list of all the pool names.
`Number of Leased Addresses`	Displays the number of leased address entries for the pool.
`Total in all Pools`	Displays the total number of leased address entries for all pools.

Example 2 To display addresses, prefixes, and lifetimes for all DHCPv6 leasing entries by pool, enter:

```
awplus# show ipv6 dhcp binding
```

Output Figure 42-6: Example output from the **show ipv6 dhcp binding** command

```
awplus#show ipv6 dhcp binding
Pool ia-na1
 Address 2002:0:3c0::1
         client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
         preferred lifetime 604800, valid lifetime 2592000
         starts  at 20 Aug 2012 18:38:29
         expires at 19 Sep 2012 18:38:29
Pool ia-pd1
 Prefix  2002:0:3c0::/42
         client IAID 77f7ba23, DUID 0001000117c4bbb4001577f7ba23
         preferred lifetime 604800, valid lifetime 2592000
         starts  at 20 Aug 2012 18:38:29
         expires at 19 Sep 2012 18:38:29
```

Table 4: Parameters in the output of the **showipv6 dhcp binding** command

Parameter	Description
`Address`	Address delegated to the indicated IAID and DUID. See the IAID and DUID descriptions below for further information.
`Prefix`	Prefix delegated to the indicated IAID and DUID. See the IAID and DUID descriptions below for further information.
`DUID`	DHCPv6 unique identifier (DUID) (see RFC 3315). Each DHCPv6 client has as DUID. DHCPv6 servers use DUIDs to identify clients for the association of IAs (Identity Associations) with DHCPv6 clients. DHCPv6 clients use DUIDs to identify a DHCPv6 server.
`IAID`	Identify Association Identifier (IAID) (see RFC 3315). IAIDs are identifiers for IAs (Identity Associations), where an IA is a collection of IPv6 addresses assigned to a DHCPv6 client. Each IA has an associated IAD. Each DHCPv6 client may have more than one IA assigned to it. Each IA holds one type of address.
`preferred lifetime`	The preferred lifetime setting in seconds for the specified IAID and DUID. Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires. Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected.
`valid lifetime`	The valid lifetime setting in seconds for the specified IAID and DUID. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.

Table 4: Parameters in the output of the **showipv6 dhcp binding** command

Parameter	Description
`starts at`	The date and time at which the valid lifetime expires.
`expires at`	The date and time at which the valid lifetime expires.

Related Commands

clear ipv6 dhcp binding

ipv6 dhcp pool

show ipv6 dhcp pool

show ipv6 dhcp interface

Overview Use this command in User Exec or Privileged Exec mode to display DHCPv6 information for a specified interface, or all interfaces when entered without the interface parameter.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax `show ipv6 dhcp interface [<interface-name>]`

Parameter	Description
<interface-name>	Optional. Specify the name of the interface to show DHCPv6 information about. Omit this optional parameter to display DHCPv6 information for all interfaces DHCPv6 is configured on.

Mode User Exec and Privileged Exec

Example1 To display DHCPv6 information for all interfaces DHCPv6 is configured on, use the command:

```
awplus# show ipv6 dhcp interface
```

Output Figure 42-7: Example output from the **show ipv6 dhcp interface** command

```
awplus# show ipv6 dhcp interface
vlan1 is in client mode
 Address 1001::3c0:1
         preferred lifetime 9000, valid lifetime 5000
         starts  at 20 Jan 2012 09:21:35
         expires at 20 Jan 2012 10:25:32
vlan2
is in client (Prefix-Delegation) mode
 Prefix
name pd1

     prefix 2002:0:3c0::/42

     preferred lifetime 604800, valid lifetime 2592000

     starts  at 20 Aug 2012 09:21:33

     expires at 19 Sep 2012 09:21:33
vlan3
is in server mode
 Using
pool  : pool-1;
 Preference:
0
```

Example 2 To display DHCPv6 information for interface vlan2, use the command:

```
awplus# show ipv6 dhcp interface vlan2
```

Output Figure 42-8: Example output from the **show ipv6 dhcp interface vlan2** command

```
awplus# show ipv6 dhcp interface vlan2
vlan2 is in client (Prefix-Delegation) mode
 Prefix name pd1
        prefix 2002:0:3c0::/42
        preferred lifetime 604800, valid lifetime 2592000
        starts  at 20 Aug 2012 09:21:33
        expires at 19 Sep 2012 09:21:33
```

Table 5: Parameters in the output of the **show counter dhcp-client** command

Parameter	Description
`<interface> is in server/client/(Prefix-Delegation) mode`	Displays whether the specified interface is in server or client mode and whether prefix-delegation is applied to an interface.
`Address`	Displays the address of the DHCPv6 server on the interface.
`Prefix name`	Displays the IPv6 general prefix pool name, where prefixes are stored for the interface.
`Using pool`	Displays the name of the pool used by the interface.
`Preference`	Displays the preference value for the DHCPv6 server.

Related Commands ipv6 dhcp client pd

show ipv6 dhcp pool

Overview Use this command in User Exec or Privileged Exec mode to display the configuration details and system usage of the DHCPv6 address pools configured on the device.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Syntax

```
show ipv6 dhcp pool [<DHCPv6-address-pool-name>]
```

Parameter	Description
<DHCPv6-address-pool-name>	Name of a specific DHCPv6 address pool. This displays the configuration of the specified DHCPv6 address pool only.

Mode User Exec and Privileged Exec

Example

```
awplus# show ipv6 dhcp pool
```

Output Figure 42-9: Example output from the **show ipv6 dhcp pool** command

```
awplus# show ipv6 dhcp pool
DHCPv6 Pool: ia-na
 Address Prefix   : 1001::/64
         Lifetime: 2592000(valid), 604800(preferred)
 DNS Server: 2001::1
 DNS Server: 2001::2
 Domain Name: example.com
 Domain Name: example.co.jp
 SNTP Server: 2001::5
 SNTP Server: 2001::6
 Option Code : 150
        Value: [ASCII] test-test
DHCPv6 Pool: ia-pd
 PD Pool Name: pd1
    Prefix    : 2002::/38-42
    Lifetime : 2592000(valid), 604800(preferred)
```

Table 6: Parameters in the output of the **show ipv6dhcp pool** command

Parameter	Description
DHCPv6 Pool	Name of the DHCPv6 pool.
Address Prefix	Address prefix to the DHCPv6 pool.

Table 6: Parameters in the output of the **show ipv6dhcp pool** command (cont.)

Parameter	Description
`Address Lifetime`	Valid and preferred lifetimes to the DHCPv6 pool. Preferred IPv6 addresses or prefixes are available to interfaces for unrestricted use and are deprecated when the preferred timer expires. Deprecated IPv6 addresses and prefixes are available for use and are discouraged but not forbidden. A deprecated address or prefix should not be used as a source address or prefix, but packets sent from deprecated addresses or prefixes are delivered as expected. An IPv6 address or prefix becomes invalid and is not available to an interface when the valid lifetime timer expires. Invalid addresses or prefixes should not appear as the source or destination for a packet.
`DNS Server`	IPv6 address of the DNS Server
`Domain name`	URL for the domain name.
`SNTP Server`	IPv6 address of the SNTP (Simple Network Time Protocol) Server.
`Option Code`	DHCP Option code (see RFC 2132).
`Option Value`	DHCP Option value type (see RFC 2132).

Related Commands ipv6 dhcp pool

sntp-address

Overview Use this command in DHCPv6 Configuration mode to add an SNTP Server IPv6 address to a DHCPv6 Server pool.

Use the **no** variant of this command to remove an SNTP Server IPv6 address from a DHCPv6 Server pool.

Syntax

```
sntp-address <ipv6-address>
no sntp-address <ipv6-address>
```

Parameter	Description
<ipv6-address>	Specify an SNTP Server IPv6 address, in hexadecimal notation in the format `X:X::X:X`.

Mode DHCPv6 Configuration

Examples The following example adds an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# sntp-address 2001:0db8::/32
```

The following example removes an SNTP Server IPv6 address of 2001:0db8::/32 to the DHCPv6 pool named P2:

```
awplus# configure terminal
awplus(config)# ipv6 dhcp pool P2
awplus(config-dhcp6)# no sntp-address 2001:0db8::/32
```

Related Commands

dns-server (DHCPv6)

domain-name (DHCPv6)

option (DHCPv6)

show ipv6 dhcp pool

43 NTP Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure the Network Time Protocol (NTP). For more information, see the NTP Feature Overview and Configuration Guide.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

ntp access-group

Overview This command creates an NTP access group, and applies a basic IP access list to it. This allows you to control access to NTP services.

The **no** variant of this command removes the configured NTP access group.

Syntax

```
ntp access-group [peer|query-only|serve|serve-only]
[<1-99>|<1300-1999>]
```

```
no ntp access-group [peer|query-only|serve|serve-only]
```

Parameter	Description
`peer`	Allows time requests and NTP control queries, and allows the system to synchronize itself to a system whose address passes the access list criteria.
`query-only`	Allows only NTP control queries from a system whose address passes the access list criteria.
`serve`	Allows time requests and NTP control queries, but does not allow the system to synchronize itself to a system whose address passes the access list criteria.
`serve-only`	Allows only time requests from a system whose address passes the access list criteria.
<1-99>	Standard IP access list.
<1300-1999>	Expanded IP access list.

Mode Global Configuration

Examples To create an NTP peer access group for an extended IP access list, use the commands:

```
awplus# configure terminal
awplus(config)# ntp access-group peer 1998
```

To disable the NTP peer access group created above, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp access-group peer
```

ntp authenticate

Overview This command enables NTP authentication. This allows NTP to authenticate the associations with other systems for security purposes.

The **no** variant of this command disables NTP authentication.

Syntax

```
ntp authenticate
no ntp authenticate
```

Mode Global Configuration

Examples To enable NTP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# ntp authenticate
```

To disable NTP authentication, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp authenticate
```

ntp authentication-key

Overview This command defines each of the authentication keys. Each key has a key number, a type, and a value. Currently, the only key type supported is MD5.

The **no** variant of this disables the authentication key assigned previously using **ntp authentication-key**.

Syntax

```
ntp authentication-key <keynumber> md5 <key>
no ntp authentication-key <keynumber> md5 <key>
```

Parameter	Description
<keynumber>	*<1-4294967295>* The key number.
<key>	The authentication key.

Mode Global Configuration

Examples To define an authentication key number `134343` and a key value `mystring`, use the commands:

```
awplus# configure terminal
awplus(config)# ntp authentication-key 134343 md5 mystring
```

To disable the authentication key number `134343` with the key value mystring, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp authentication-key 134343 md5 mystring
```

ntp broadcastdelay

Overview Use this command to set the estimated round-trip delay for broadcast packets.

Use the **no** variant of this command to reset the round-trip delay for broadcast packets to the default offset of 0 microseconds.

Syntax

```
ntp broadcastdelay <delay>
no ntp broadcastdelay
```

Parameter	Description
<delay>	*<1-999999>* The broadcast delay in microseconds.

Default 0 microsecond offset, which can only be applied with the **no** variant of this command.

Mode Global Configuration

Examples To set the estimated round-trip delay to 23464 microseconds for broadcast packets, use these commands:

```
awplus# configure terminal
awplus(config)# ntp broadcastdelay 23464
```

To reset the estimated round-trip delay for broadcast packets to the default setting (0 microseconds), use these commands:

```
awplus# configure terminal
awplus(config)# no ntp broadcastdelay
```

ntp master

Overview Use this command to make the device to be an authoritative NTP server, even if the system is not synchronized to an outside time source. Note that no stratum number is set by default.

Use the **no** variant of this command to stop the device being the designated NTP server.

Syntax

```
ntp master [<stratum>]
no ntp master
```

Parameter	Description
<stratum>	*<1-15>* The stratum number defines the configured level that is set for this master within the NTP hierarchy.

Mode Global Configuration

Usage The stratum number is null by default and must be set using this command. The stratum levels define the distance from the reference clock and exist to prevent cycles in the hierarchy. Stratum 1 is used to indicate time servers, which are more accurate than Stratum 2 servers. For more information on the Network Time Protocol go to: www.ntp.org

Examples To stop the device from being the designated NTP server use the commands:

```
awplus# configure terminal
awplus(config)# no ntp master
```

To make the device the designated NTP server with stratum number 2 use the commands:

```
awplus# configure terminal
awplus(config)# ntp master 2
```

ntp peer

Overview Use this command to configure an NTP peer association. An NTP association is a peer association if this system is willing to either synchronize to the other system, or allow the other system to synchronize to it.

Use the **no** variant of this command to remove the configured NTP peer association.

Syntax

```
ntp peer {<peeraddress>|<peername>}
ntp peer {<peeraddress>|<peername>} [prefer] [key <key>] [version <version>]
no ntp peer {<peeraddress>|<peername>}
```

Parameter	Description
<peeraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X:X`for an IPv6 address.
<peername>	Specify the peer hostname. The peer hostname can resolve to an IPv4 and an IPv6 address.
`prefer`	Prefer this peer when possible.
`key <key>`	*<1-4294967295>* Configure the peer authentication key.
`version <version>`	*<1-4>* Configure for this NTP version.

Mode Global Configuration

Examples See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv4 address of `192.0.2.23`:

```
awplus# configure terminal
awplus(config)# ntp peer 192.0.2.23
awplus(config)# ntp peer 192.0.2.23 prefer
awplus(config)# ntp peer 192.0.2.23 prefer version 4
awplus(config)# ntp peer 192.0.2.23 prefer version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4 key 1234
awplus(config)# ntp peer 192.0.2.23 version 4
awplus(config)# ntp peer 192.0.2.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of `192.0.2.23`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 192.0.2.23
```

See the following commands for options to configure NTP peer association, key and NTP version for the peer with an IPv6 address of 2001:0db8:010d::1:

```
awplus# configure terminal
awplus(config)# ntp peer 2001:0db8:010d::1
awplus(config)# ntp peer 2001:0db8:010d::1 prefer
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4
awplus(config)# ntp peer 2001:0db8:010d::1 prefer version 4 key
1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4 key 1234
awplus(config)# ntp peer 2001:0db8:010d::1 version 4
awplus(config)# ntp peer 2001:0db8:010d::1 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010d::1, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp peer 2001:0db8:010d::1
```

Related Commands

ntp server

ntp source

ntp server

Overview Use this command to configure an NTP server. This means that this system will synchronize to the other system, and not vice versa.

Use the **no** variant of this command to remove the configured NTP server.

Syntax

```
ntp server {<serveraddress>|<servername>}
ntp server {<serveraddress>|<servername>} [prefer] [key <key>] [version <version>]
no ntp server {<serveraddress>|<servername>}
```

Parameter	Description
<serveraddress>	Specify the IP address of the peer, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X` for an IPv6 address.
<servername>	Specify the server hostname. The server hostname can resolve to an IPv4 and an IPv6 address.
`prefer`	Prefer this server when possible.
`key <key>`	*<1-4294967295>* Configure the server authentication key.
`version <version>`	*<1-4>* Configure for this NTP version.

Mode Global Configuration

Examples See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv4 address of 192.0.1.23:

```
awplus# configure terminal
awplus(config)# ntp server 192.0.1.23
awplus(config)# ntp server 192.0.1.23 prefer
awplus(config)# ntp server 192.0.1.23 prefer version 4
awplus(config)# ntp server 192.0.1.23 prefer version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4 key 1234
awplus(config)# ntp server 192.0.1.23 version 4
awplus(config)# ntp server 192.0.1.23 key 1234
```

To remove an NTP peer association for this peer with an IPv4 address of 192.0.1.23, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp server 192.0.1.23
```

See the following commands for options to configure an NTP server association, key and NTP version for the server with an IPv6 address of 2001:0db8:010e::2:

```
awplus# configure terminal
awplus(config)# ntp server 2001:0db8:010e::2
awplus(config)# ntp server 2001:0db8:010e::2 prefer
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
awplus(config)# ntp server 2001:0db8:010e::2 prefer version 4
key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4 key 1234
awplus(config)# ntp server 2001:0db8:010e::2 version 4
awplus(config)# ntp server 2001:0db8:010e::2 key 1234
```

To remove an NTP peer association for this peer with an IPv6 address of 2001:0db8:010e::2, use the commands:

```
awplus# configure terminal
awplus(config)# no ntp server 2001:0db8:010e::2
```

Related Commands

ntp peer

ntp source

ntp source

Overview Use this command to configure an IPv4 or an IPv6 address for the NTP source interface. This command defines the socket used for NTP messages, and only applies to NTP client behavior.

Use the **no** variant of this command to remove the configured IPv4 or IPv6 address from the NTP source interface.

Syntax

```
ntp source <source-address>
no ntp source
```

Parameter	Description
<source-address>	Specify the IP address of the NTP source interface, entered in the form `A.B.C.D` for an IPv4 address, or in the form `X:X::X.X`for an IPv6 address.

Default An IP address is selected based on the most appropriate egress interface used to reach the NTP peer if a configured NTP client source IP address is unavailable or is an invalid IP address.

Mode Global Configuration

Usage Adding an IPv4 or an IPv6 address allows you to select which source interface NTP uses for peering. The IPv4 or IPv6 address configured using this command is matched to the interface.

When selecting a source IP address to use for NTP messages to the peer, if the configured NTP client source IP address is unavailable then default behavior will apply, and an alternative source IP address is automatically selected. This IP address is based on the most appropriate egress interface used to reach the NTP peer. The configured NTP client source IP may be unavailable if the interface is down, or an invalid IP address is configured that does not reside on the device.

Note that this command only applies to NTP client behavior. The egress interface that the NTP messages use to reach the NTP server determined by the ntp peer and ntp server commands.

Examples To configure the NTP source interface with the IPv4 address `192.0.2.23`, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 192.0.2.23
```

To configure the NTP source interface with the IPv6 address `2001:0db8:010e::2`, enter the commands:

```
awplus# configure terminal
awplus(config)# ntp source 2001:0db8:010e::2
```

To remove a configured address for the NTP source interface, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp source
```

Related Commands

ntp peer

ntp server

ntp trusted-key

Overview This command defines a list of trusted authentication keys. If a key is trusted, this system will be ready to synchronize to a system that uses this key in its NTP packets.

Use the **no** variant of this command to remove a configured trusted authentication key.

Syntax

```
ntp trusted-key <1-4294967295>
no ntp trusted-key <1-4294967295>
```

Parameter	Description
<1-4294967295>	The specific key number.

Mode Global Configuration

Examples To define a trusted authentication key numbered 234675, use the following commands:

```
awplus# configure terminal
awplus(config)# ntp trusted-key 234676
```

To remove the trusted authentication key numbered `234675`, use the following commands:

```
awplus# configure terminal
awplus(config)# no ntp trusted-key 234676
```

show counter ntp

Overview This command displays packet counters for NTP.

Syntax

```
show counter ntp
```

Mode User Exec and Privileged Exec

Example To display counters for NTP use the command:

```
awplus# show counter ntp
```

Figure 43-1: Example output from **show counter ntp**

```
NTP counters
Pkts Sent               ......... 0
Pkts Received           ......... 70958
Pkts Processed          ......... 0
Pkts current version    ......... 0
Pkts old version        ......... 0
Pkts unknown version    ......... 0
Pkts access denied      ......... 70958
Pkts bad length         ......... 0
Pkts bad auth           ......... 0
Pkts rate exceed        ......... 0
```

Table 43-1: Parameters in the output from **show counter ntp**

Parameter	Description
Pkts Sent	Total number of NTP client and server packets sent by your device.
Pkts Received	Total number of NTP client and server packets received by your device.
Pkts Processed	The number of packets processed by NTP. NTP processes a packet once it has determined that the packet is valid by checking factors such as the packet's authentication, format, access rights and version.
Pkts current version	The number of version 4 NTP packets received.
Pkts old version	The number of NTP packets received that are from an older version, down to version 1, of NTP. NTP is compatible with these versions and processes these packets.
Pkts unknown version	The number of NTP packets received that are an earlier version than version 1, or a higher version than version 4. NTP cannot process these packets.

Table 43-1: Parameters in the output from **show counter ntp** (cont.)

Parameter	Description
`Pkts access denied`	The number of NTP packets received that do not match any access list statements in the NTP access-groups. NTP drops these packets.
`Pkts bad length`	The number of NTP packets received that do not conform to the standard packet length. NTP drops these packets.
`Pkts bad auth`	The number of NTP packets received that failed authentication. NTP drops these packets. Packets can only fail authentication if NTP authentication is enabled with the ntp authenticate command.
`Pkts rate exceed`	The number of packets dropped because the packet rate exceeded its limits.

show ntp associations

Overview Use this command to display the status of NTP associations. Use the detail option for displaying detailed information about the associations.

Syntax `show ntp associations [detail]`

Mode User Exec and Privileged Exec

Example See the sample output of the **show ntp associations** and **show ntp associations detail** commands displaying the status of NTP associations.

Table 44: Example output from the **show ntp associations** command

```
awplus#show ntp associations
  address          ref clock       st  when  poll reach   delay  offset    disp
 ~192.0.2.23       INIT            16     -   512   000     0.0     0.0     0.0
 * master (synced), # master (unsynced), + selected, - candidate, ~ configured
awplus#
```

Table 45: Example output from the **show ntp associations detail** command

```
awplus#show ntp associations detail
192.0.2.23 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 (06:28:16.000 UTC Thu Feb  7 2036)
our mode client, peer mode unspec, our poll intvl 512, peer poll intvl 1024
root delay 0.00 msec, root disp 0.00, reach 000,
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-19,
org time 00000000.00000000 (06:28:16.000 UTC Thu Feb  7 2036)
rcv time 00000000.00000000 (06:28:16.000 UTC Thu Feb  7 2036)
xmt time cf11f2a4.cedde5e4 (00:39:00.808 UTC Tue Feb  2 2010)
filtdelay =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filtoffset =  0.00  0.00  0.00  0.00  0.00  0.00  0.00  0.00
filterror =  16000.00  16000.00  16000.00  16000.00  16000.00  16000.00  16000.0
0  16000.00
```

Table 46: Parameters in the output from the **show ntp associations** command

Parameter	Description
`address`	Peer IP address
`ref clock`	IP address for reference clock
`st`	Stratum. The number of hops between the server and the accurate time source.
`poll`	Time between NTP requests from the device to the server.

Table 46: Parameters in the output from the **show ntp associations** command

Parameter	Description
`reach`	Shows whether or not the NTP server responded to the last request.
`delay`	Round trip delay between the device and the server.
`offset`	Difference between the device clock and the server clock.
`disp`	Lowest measure of error associated with peer offset based on delay.

show ntp status

Overview Use this command to display the status of the Network Time Protocol (NTP).

Syntax

```
show ntp status
```

Mode User Exec and Privileged Exec

Example See the sample output of the **show ntp status** command displaying information about the Network Time Protocol.

Figure 43-2: Example output from the **show ntp status** command

```
awplus#sh ntp status
Clock is synchronized, stratum 3, reference is 127.127.1.0
actual frequency is 0.0000 Hz, precision is 2**-19
reference time is cf11f3f2.c7c081a1 (00:44:34.780 UTC Tue Feb  2
2010)
clock offset is 0.000 msec, root delay is 0.000 msec
root dispersion is 7947729.000 msec,
awplus#
```

44 SNMP Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure SNMP. For more information, see:

- the Support for Allied Telesis Enterprise_MIBs in AlliedWare Plus, for information about which MIB objects are supported.
- the SNMP Feature Overview and Configuration_Guide.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

debug snmp

Overview This command enables SNMP debugging.

The **no** variant of this command disables SNMP debugging.

Syntax

```
debug snmp
[all|detail|error-string|process|receive|send|xdump]
```

```
no debug snmp
[all|detail|error-string|process|receive|send|xdump]
```

Parameter	Description
`all`	Enable or disable the display of all SNMP debugging information.
`detail`	Enable or disable the display of detailed SNMP debugging information.
`error-string`	Enable or disable the display of debugging information for SNMP error strings.
`process`	Enable or disable the display of debugging information for processed SNMP packets.
`receive`	Enable or disable the display of debugging information for received SNMP packets.
`send`	Enable or disable the display of debugging information for sent SNMP packets.
`xdump`	Enable or disable the display of hexadecimal dump debugging information for SNMP packets.

Mode Privileged Exec and Global Configuration

Example To start SNMP debugging, use the command:

```
awplus# debug snmp
```

To start SNMP debugging, showing detailed SNMP debugging information, use the command:

```
awplus# debug snmp detail
```

To start SNMP debugging, showing all SNMP debugging information, use the command:

```
awplus# debug snmp all
```

Related Commands

show debugging snmp

terminal monitor

undebug snmp

show counter snmp-server

Overview This command displays counters for SNMP messages received by the SNMP agent.

Syntax

```
show counter snmp-server
```

Mode User Exec and Privileged Exec

Example To display the counters for the SNMP agent, use the command:

```
awplus# show counter snmp-server
```

Output Figure 44-1: Example output from the **show counter snmp-server** command

```
SNMP-SERVER counters
inPkts                ......... 11
inBadVersions         ......... 0
inBadCommunityNames   ......... 0
inBadCommunityUses    ......... 0
inASNParseErrs        ......... 0
inTooBigs             ......... 0
inNoSuchNames         ......... 0
inBadValues           ......... 0
inReadOnlys           ......... 0
inGenErrs             ......... 0
inTotalReqVars        ......... 9
inTotalSetVars        ......... 0
inGetRequests         ......... 2
inGetNexts            ......... 9
inSetRequests         ......... 0
inGetResponses        ......... 0
inTraps               ......... 0
outPkts               ......... 11
outTooBigs            ......... 0
outNoSuchNames        ......... 2
outBadValues          ......... 0
outGenErrs            ......... 0
outGetRequests        ......... 0
outGetNexts           ......... 0
outSetRequests        ......... 0
outGetResponses       ......... 11
outTraps              ......... 0
UnSupportedSecLevels  ......... 0
NotInTimeWindows      ......... 0
UnknownUserNames      ......... 0
UnknownEngineIDs      ......... 0
WrongDigest           ......... 0
DecryptionErrors      ......... 0
UnknownSecModels      ......... 0
InvalidMsgs           ......... 0
UnknownPDUHandlers    ......... 0
```

Table 1: Parameters in the output of the **show counter snmp-server** command

Parameter	Meaning
inPkts	The total number of SNMP messages received by the SNMP agent.
inBadVersions	The number of messages received by the SNMP agent for an unsupported SNMP version. It drops these messages.The SNMP agent on your device supports versions 1, 2C, and 3.
inBadCommunityNames	The number of messages received by the SNMP agent with an unrecognized SNMP community name. It drops these messages.
inBadCommunityUses	The number of messages received by the SNMP agent where the requested SNMP operation is not permitted from SNMP managers using the SNMP community named in the message.
inASNParseErrs	The number of ASN.1 or BER errors that the SNMP agent has encountered when decoding received SNMP Messages.
inTooBigs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'tooBig'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inNoSuchNames	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'noSuchName'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inBadValues	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'badValue'. This is sent by an SNMP manager to indicate that an exception occurred when processing a request from the agent.
inReadOnlys	The number of valid SNMP PDUs received by the SNMP agent where the value of the error-status field is 'readOnly'. The SNMP manager should not generate a PDU which contains the value 'readOnly' in the error-status field. This indicates that there is an incorrect implementations of the SNMP.
inGenErrs	The number of SNMP PDUs received by the SNMP agent where the value of the error-status field is 'genErr'.

Table 1: Parameters in the output of the **show counter snmp-server** command

Parameter	Meaning
inTotalReqVars	The number of MIB objects that the SNMP agent has successfully retrieved after receiving valid SNMP Get-Request and Get-Next PDUs.
inTotalSetVars	The number of MIB objects that the SNMP agent has successfully altered after receiving valid SNMP Set-Request PDUs.
inGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has accepted and processed.
inGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has accepted and processed.
inSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has accepted and processed.
inGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has accepted and processed.
inTraps	The number of SNMP Trap PDUs that the SNMP agent has accepted and processed.
outPkts	The number of SNMP Messages that the SNMP agent has sent.
outTooBigs	The number of SNMP PDUs that the SNMP agent has generated with the value 'tooBig' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outNoSuchNames	The number of SNMP PDUs that the SNMP agent has generated with the value `noSuchName' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outBadValues	The number of SNMP PDUs that the SNMP agent has generated with the value 'badValue' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGenErrs	The number of SNMP PDUs that the SNMP agent has generated with the value 'genErr' in the error-status field. This is sent to the SNMP manager to indicate that an exception occurred when processing a request from the manager.
outGetRequests	The number of SNMP Get-Request PDUs that the SNMP agent has generated.

Table 1: Parameters in the output of the **show counter snmp-server** command

Parameter	Meaning
outGetNexts	The number of SNMP Get-Next PDUs that the SNMP agent has generated.
outSetRequests	The number of SNMP Set-Request PDUs that the SNMP agent has generated.
outGetResponses	The number of SNMP Get-Response PDUs that the SNMP agent has generated.
outTraps	The number of SNMP Trap PDUs that the SNMP agent has generated.
UnSupportedSecLevels	The number of received packets that the SNMP agent has dropped because they requested a securityLevel unknown or not available to the SNMP agent.
NotInTimeWindows	The number of received packets that the SNMP agent has dropped because they appeared outside of the authoritative SNMP agent's window.
UnknownUserNames	The number of received packets that the SNMP agent has dropped because they referenced an unknown user.
UnknownEngineIDs	The number of received packets that the SNMP agent has dropped because they referenced an unknown snmpEngineID.
WrongDigest	The number of received packets that the SNMP agent has dropped because they didn't contain the expected digest value.
DecryptionErrors	The number of received packets that the SNMP agent has dropped because they could not be decrypted.
UnknownSecModels	The number of messages received that contain a security model that is not supported by the server. Valid for SNMPv3 messages only.
InvalidMsgs	The number of messages received where the security model is supported but the authentication fails. Valid for SNMPv3 messages only.
UnknownPDUHandlers	The number of times the SNMP handler has failed to process a PDU. This is a system debugging counter.

Related Commands show snmp-server

show debugging snmp

Overview This command displays whether SNMP debugging is enabled or disabled.

Syntax

```
show debugging snmp
```

Mode User Exec and Privileged Exec

Example To display the status of SNMP debugging, use the command:

```
awplus# show debugging snmp
```

Output Figure 44-2: Example output from the **show debugging snmp** command

```
Snmp (SMUX) debugging status:
  Snmp debugging is on
```

Related Commands debug snmp

show running-config snmp

Overview This command displays the current configuration of SNMP on your device.

Syntax

```
show running-config snmp
```

Mode Privileged Exec

Example To display the current configuration of SNMP on your device, use the command:

```
awplus# show running-config snmp
```

Output Figure 44-3: Example output from the **show running-config snmp** command

```
snmp-server contact AlliedTelesis
snmp-server location Philippines
snmp-server group grou1 auth read view1 write view1 notify view1
snmp-server view view1 1 included
snmp-server community public
snmp-server user user1 group1 auth md5 password priv des
password
```

Related Commands show snmp-server

show snmp-server

Overview This command displays the status and current configuration of the SNMP server.

Syntax

```
show snmp-server
```

Mode Privileged Exec

Example To display the status of the SNMP server, use the command:

```
awplus# show snmp-server
```

Output Figure 44-4: Example output from the **show snmp-server** command

```
SNMP Server ......................... Enabled
IP Protocol ......................... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ............ 0x80001f888021338e4747b8e607
```

Related Commands

debug snmp

show counter snmp-server

snmp-server

snmp-server engineID local

snmp-server engineID local reset

show snmp-server community

Overview This command displays the SNMP server communities configured on the device. SNMP communities are specific to v1 and v2c.

Syntax

```
show snmp-server community
```

Mode Privileged Exec

Example To display the SNMP server communities, use the command:

```
awplus# show snmp-server community
```

Output Figure 44-5: Example output from the **show snmp-server community** command

```
SNMP community information:
  Community Name ........... public
    Access ................. Read-only
    View ................... none
```

Related Commands

show snmp-server

snmp-server community

show snmp-server group

Overview This command displays information about SNMP server groups. This command is used with SNMP version 3 only.

Syntax

```
show snmp-server group
```

Mode Privileged Exec

Example To display the SNMP groups configured on the device, use the command:

```
awplus# show snmp-server group
```

Output Figure 44-6: Example output from the **show snmp-server group** command

```
SNMP group information:
  Group name ............... guireadgroup
    Security Level ........ priv
    Read View ............. guiview
    Write View ............ none
    Notify View ........... none

  Group name ............... guiwritegroup
    Security Level ........ priv
    Read View ............. none
    Write View ............ guiview
    Notify View ........... none
```

Related Commands show snmp-server

snmp-server group

show snmp-server user

Overview This command displays the SNMP server users and is used with SNMP version 3 only.

Syntax

```
show snmp-server user
```

Mode Privileged Exec

Example To display the SNMP server users configured on the device, use the command:

```
awplus# show snmp-server user
```

Output Figure 44-7: Example output from the **show snmp-server user** command

```
Name                Group name          Auth        Privacy
-------             -------------       -------     ----------
freddy              guireadgroup        none        none
```

Related Commands

show snmp-server

snmp-server user

show snmp-server view

Overview This command displays the SNMP server views and is used with SNMP version 3 only.

Syntax
```
show snmp-server view
```

Mode Privileged Exec

Example To display the SNMP server views configured on the device, use the command:

```
awplus# show snmp-server view
```

Output Figure 44-8: Example output from the **show snmp-server view** command

```
SNMP view information:
  View Name ............... view1
    OID ..................... 1
    Type .................... included
```

Related Commands
show snmp-server

snmp-server view

snmp trap link-status

Overview Use this command to enable SNMP to send link status notifications (traps) for the interfaces when an interface goes up (linkUp) or down (linkDown).

Use the **no** variant of this command to disable the sending of link status notifications.

Syntax

```
snmp trap link-status [enterprise]
no snmp trap link-status
```

Parameter	Description
`enterprise`	Send an Allied Telesis enterprise type of link trap.

Default By default, link status notifications are disabled.

Mode Interface Configuration

Usage The link status notifications can be enabled for the following interface types:

- switch port (e.g. port 1.0.1)
- VLAN (e.g. vlan2)
- static and dynamic link aggregation (e.g. sa2, po2)

To specify where notifications are sent, use the snmp-server host command. To configure the device globally to send other notifications, use the snmp-server enable trap command.

Examples To enable SNMP to send link status notifications for ports 1.0.2 to 1.0.6, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2-1.0.6
awplus(config-if)# snmp trap link-status
```

To enable SNMP to send an Allied Telesis enterprise type of link status notification for port1.0.1, use following commands:

```
awplus# configure terminal
awplus(config)# interface 1.0.1
awplus(config-if)# snmp trap link-status enterprise
```

To disable the sending of link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no snmp trap link-status
```

Related Commands

show interface

snmp trap link-status suppress

snmp-server enable trap

snmp-server host

snmp trap link-status suppress

Overview Use this command to enable the suppression of link status notifications (traps) for the interfaces beyond the specified threshold, in the specified interval.

Use the **no** variant of this command to disable the suppression of link status notifications for the ports.

Syntax

```
snmp trap link-status suppress {time {<1-60>|default}|threshold
{<1-20>|default}}
```

```
no snmp trap link-status suppress
```

Parameter	Description
`time`	Set the suppression timer for link status notifications.
<1-60>	The suppress time in seconds.
`default`	The default suppress time in seconds (60).
`threshold`	Set the suppression threshold for link status notifications. This is the number of link status notifications after which to suppress further notifications within the suppression timer interval.
<1-20>	The number of link status notifications.
`default`	The default number of link status notifications (20).

Default By default, if link status notifications are enabled (they are enabled by default), the suppression of link status notifications is enabled: notifications that exceed the notification threshold (default 20) within the notification timer interval (default 60 seconds) are not sent.

Mode Interface Configuration

Usage An unstable network can generate many link status notifications. When notification suppression is enabled, a suppression timer is started when the first link status notification of a particular type (linkUp or linkDown) is sent for an interface. If the threshold number of notifications of this type is sent before the timer reaches the suppress time, any further notifications of this type generated for the interface during the interval are not sent. At the end of the interval, the sending of link status notifications resumes, until the threshold is reached in the next interval.

Examples To enable the suppression of link status notifications for ports 1.0.2 to 1.0.6 after 10 notifications have been sent in 40 seconds, use following commands:

```
awplus# configure terminal
```

```
awplus(config)# interface port1.0.2-1.0.6
```

```
awplus(config-if)# snmp trap link-status suppress time 40
threshold 10
```

To disable the suppression link status notifications for port 1.0.2, use following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no snmp trap link-status suppress
```

Related Commands

show interface

snmp trap link-status

snmp-server

Overview Use this command to enable the SNMP agent (server) on the device. The SNMP agent receives and processes SNMP packets sent to the device, and generates notifications (traps) that have been enabled by the snmp-server enable trap command.

Use the **no** variant of this command to disable the SNMP agent on the device. When SNMP is disabled, SNMP packets received by the device are discarded, and no notifications are generated. This does not remove any existing SNMP configuration.

Syntax

```
snmp-server [ip|ipv6]
no snmp-server [ip|ipv6]
```

Parameter	Description
ip	Enable or disable the SNMP agent for IPv4.
ipv6	Enable or disable the SNMP agent for IPv6.

Default By default, the SNMP agent is enabled for both IPv4 and IPv6. If neither the **ip** parameter nor the **ipv6** parameter is specified for this command, then SNMP is enabled or disabled for both IPv4 and IPv6.

Mode Global Configuration

Examples To enable SNMP on the device for both IPv4 and IPv6, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server
```

To enable the SNMP agent for IPv4 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server ip
```

To disable the SNMP agent for both IPv4 and IPv6 on the device, use the commands:

```
awplus# configure terminal
awplus(config)# no snmp-server
```

To disable the SNMP agent for IPv4, use the commands:

```
awplus(config)# no snmp-server ipv4
```

Related Commands

show snmp-server

show snmp-server community

show snmp-server user

snmp-server community

snmp-server contact

snmp-server enable trap

snmp-server engineID local

snmp-server group

snmp-server host

snmp-server location

snmp-server view

snmp-server community

Overview This command creates an SNMP community, optionally setting the access mode for the community. The default access mode is read only. If view is not specified, the community allows access to all the MIB objects. The SNMP communities are only valid for SNMPv1 and v2c and provide very limited security. Communities should not be used when operating SNMPv3.

The **no** variant of this command removes an SNMP community. The specified community must already exist on the device.

Syntax

```
snmp-server community <community-name> {view
<view-name>|ro|rw|<access-list>}
```

```
no snmp-server community <community-name> [{view
<view-name>|<access-list>}]
```

Parameter	Description
<community-name>	Community name. The community name is a case sensitive string of up to 20 characters.
`view`	Configure SNMP view. If view is not specified, the community allows access to all the MIB objects.
<view-name>	View name. The view name is a string up to 20 characters long and is case sensitive.
`ro`	Read-only community.
`rw`	Read-write community.
<access-list>	*<1-99>* Access list number.

Mode Global Configuration

Example The following command creates an SNMP community called “public” with read only access to all MIB variables from any management station.

```
awplus# configure terminal
awplus(config)# snmp-server community public ro
```

The following command removes an SNMP community called “public”

```
awplus# configure terminal
awplus(config)# no snmp-server community public
```

Related Commands

show snmp-server

show snmp-server community

snmp-server view

snmp-server contact

Overview This command sets the contact information for the system. The contact name is:

- displayed in the output of the show system command
- stored in the MIB object sysContact

The **no** variant of this command removes the contact information from the system.

Syntax

```
snmp-server contact <contact-info>
no snmp-server contact
```

Parameter	Description
<contact-info>	The contact information for the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the system contact information to "support@alliedtelesis.co.nz", use the command:

```
awplus# configure terminal
awplus(config)# snmp-server contact
support@alliedtelesis.co.nz
```

Related Commands

show system

snmp-server location

snmp-server group

snmp-server enable trap

Overview Use this command to enable the switch to transmit the specified notifications (traps).

Note that the Environmental Monitoring traps defined in the AT-ENVMONv2-MIB are enabled by default.

Use the **no** variant of this command to disable the transmission of the specified notifications.

Syntax

```
snmp-server enable trap {[atmf]
[atmflink] [atmfnode] [atmfrr] [auth] [dhcpsnooping]
[epsr] [lldp] [loopprot] [mstp] [nsm] [ospf]
[pim] [power-inline] [qsp] [rmon] [thrash-limit] [vcs] [vrrp]}

no snmp-server enable trap {[atmf]
[atmflink] [atmfnode] [atmfrr] [auth] [dhcpsnooping]
[epsr] [lldp] [loopprot] [mstp] [nsm] [ospf]
[pim] [power-inline] [qsp] [rmon] [thrash-limit] [vcs] [vrrp]}
```

Parameter	Description
`atmf`	AMF traps.
`atmflink`	AMF Link traps.
`atmfnode`	AMF Node traps.
`atmfrr`	AMF Reboot Rolling traps.
`auth`	Authentication failure.
`dhcpsnooping`	DHCP snooping and ARP security traps. These notifications must also be set using the ip dhcp snooping violation command, and/or the arp security violation command.
`epsr`	EPSR traps.
`lldp`	Link Layer Discovery Protocol (LLDP) traps. These notifications must also be enabled using the lldp notifications command, and/or the lldp med-notifications command.
`loopprot`	Loop Protection traps.
`mstp`	MSTP traps.
`nsm`	NSM traps.
`ospf`	OSPF traps.
`pim`	PIM traps.
`power-inline`	Power-inline traps (Power Ethernet MIB RFC 3621).
`qsp`	QoS Storm Protection
`rmon`	RMON traps.
`thrash-limit`	MAC address Thrash Limiting traps.

Parameter	Description
vcs	VCS traps.
vrrp	Virtual Router Redundancy (VRRP) traps.

Default By default, no notifications are generated.

Mode Global Configuration

Usage This command cannot be used to enable link status notifications globally. To enable link status notifications for particular interfaces, use the snmp trap link-status command.

To specify where notifications are sent, use the snmp-server host command.

Note that more than one trap can be configured with one command entry, and also note this command applied to notifications send by SNMP version 3.

Examples To enable the device to send a notification if an AMF node changes its status, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap atmfnode
```

To enable the device to send PoE related traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap power-inline
```

To disable PoE traps being sent out by the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable power-inline
```

To enable the device to send MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap thrash-limit
```

To disable the device from sending MAC address Thrash Limiting traps, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap thrash-limit
```

To enable the device to send OSPF and VRRP-related traps, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server enable trap ospf vrrp
```

To disable OSPF traps being sent out by the device, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server enable trap ospf
```

Related Commands

show snmp-server

show ip dhcp snooping

snmp trap link-status

snmp-server host

snmp-server engineID local

Overview Use this command to configure the SNMPv3 engine ID. The SNMPv3 engine ID is used to uniquely identify the SNMPv3 agent on a device when communicating with SNMP management clients. Once an SNMPv3 engine ID is assigned, this engine ID is permanently associated with the device until you change it.

Use the **no** variant of this command to set the user defined SNMPv3 engine ID to a system generated pseudo-random value by resetting the SNMPv3 engine. The **no snmp-server engineID local** command has the same effect as the **snmp-server engineID local default** command. Note that the snmp-server engineID local reset command is used to force the system to generate a new engine ID when the current engine ID is also system generated.

Syntax

```
snmp-server engineID local {<engine-id>|default}
no snmp-server engineID local
```

Parameter	Description
<engine-id>	Specify SNMPv3 Engine ID value, a string of up to 27 characters.
`default`	Set SNMPv3 engine ID to a system generated value by resetting the SNMPv3 engine, provided the current engine ID is user defined. If the current engine ID is system generated, use the snmp-server engineID local reset command to force the system to generate a new engine ID.

Mode Global Configuration

Usage All devices must have a unique engine ID which is permanently set unless it is configured by the user.

In a stacked environment, if the same engine ID was automatically generated for all members of the stack, conflicts would occur if the stack was dismantled. Therefore, each member of the stack will generate its own engine ID and the stack master's ID is used when transmitting SNMPv3 packets. Should a master failover occur, a different engine ID is transmitted. You can modify this behavior by manually assigning all stack members the same engine ID using the snmp-server engineID local command. However, should you decide to separate the stack and use the devices individually, you must remember to change or remove this configuration to prevent conflicts.

Example To set the SNMPv3 engine ID to 800000cf030000cd123456, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local
800000cf030000cd123456
```

To set a user defined SNMPv3 engine ID back to a system generated value, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server engineID local
```

Output The following example shows the engine ID values after configuration:

```
awplus(config)#snmp-server engineid local asdgdfh231234d
awplus(config)#exit
awplus#show snmp-server

SNMP Server ........................... Enabled
IP Protocol ........................... IPv4
SNMPv3 Engine ID (configured name) ... asdgdfh231234d
SNMPv3 Engine ID (actual) ............ 0x80001f888029af52e149198483

awplus(config)#no snmp-server engineid local
awplus(config)#exit
awplus#show snmp-server

SNMP Server ........................... Enabled
IP Protocol ........................... IPv4
SNMPv3 Engine ID (configured name) ... Not set
SNMPv3 Engine ID (actual) ............ 0x80001f888029af52e149198483
```

Validation Commands show snmp-server

Related Commands snmp-server engineID local reset

snmp-server group

snmp-server engineID local reset

Overview Use this command to force the device to generate a new pseudo-random SNMPv3 engine ID by resetting the SNMPv3 engine. If the current engine ID is user defined, use the snmp-server engineID local command to set SNMPv3 engine ID to a system generated value.

Syntax

```
snmp-server engineID local reset
```

Mode Global Configuration

Example To force the SNMPv3 engine ID to be reset to a system generated value, use the commands:

```
awplus# configure terminal
awplus(config)# snmp-server engineID local reset
```

Validation Commands show snmp-server

Related Commands snmp-server engineID local

snmp-server group

Overview This command is used with SNMP version 3 only, and adds an SNMP group, optionally setting the security level and view access modes for the group. The security and access views defined for the group represent the minimum required of its users in order to gain access.

The **no** variant of this command deletes an SNMP group, and is used with SNMPv3 only. The group with the specified authentication/encryption parameters must already exist.

Syntax

```
snmp-server group <groupname> {auth|noauth|priv} [read
<readname>|write <writename>|notify <notifyname>]
```

```
no snmp-server group <groupname> {auth|noauth|priv}
```

Parameter	Description
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
`auth`	Authentication.
`noauth`	No authentication and no encryption.
`priv`	Authentication and encryption.
`read`	Configure read view.
<readname>	Read view name.
`write`	Configure write view.
<writename>	Write view name. The view name is a string up to 20 characters long and is case sensitive.
`notify`	Configure notify view.
<notifyname>	Notify view name. The view name is a string up to 20 characters long and is case sensitive.

Mode Global Configuration

Examples To add SNMP group, for ordinary users, user the following commands:

```
awplus# configure terminal
```

```
awplus(config)# snmp-server group usergroup noauth read
useraccess write useraccess
```

To delete SNMP group `usergroup`, use the following commands

```
awplus# configure terminal
```

```
awplus(config)# no snmp-server group usergroup noauth
```

Related Commands

snmp-server

show snmp-server

show snmp-server group

show snmp-server user

snmp-server host

Overview This command specifies an SNMP trap host destination to which Trap or Inform messages generated by the device are sent.

For SNMP version 1 and 2c you must specify the community name parameter. For SNMP version 3, specify the authentication/encryption parameters and the user name. If the version is not specified, the default is SNMP version 1. Inform messages can be sent instead of traps for SNMP version 2c and 3.

Use the **no** variant of this command to remove an SNMP trap host. The trap host must already exist.

The trap host is uniquely identified by:

- host IP address (IPv4 or IPv6),
- inform or trap messages,
- community name (SNMPv1 or SNMP v2c) or the authentication/encryption parameters and user name (SNMP v3).

Syntax

```
snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
[version 1] <community-name>]
```

```
snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 2c <community-name>
```

```
snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>
```

```
no snmp-server host {<ipv4-address>|<ipv6-address>} [traps]
[version 1] <community-name>
```

```
no snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 2c <community-name>
```

```
no snmp-server host {<ipv4-address>|<ipv6-address>}
[informs|traps] version 3 {auth|noauth|priv} <user-name>
```

Parameter	Description
<ipv4-address>	IPv4 trap host address in the format A.B.C.D, for example, 192.0.2.2.
<ipv6-address>	IPv6 trap host address in the format x:x::x:x for example, 2001:db8::8a2e:7334.
informs	Send Inform messages to this host.
traps	Send Trap messages to this host (default).
version	SNMP version to use for notification messages. Default: version 1.
1	Use SNMPv1 (default).
2c	Use SNMPv2c.
3	Use SNMPv3.

Parameter	Description
`auth`	Authentication.
`noauth`	No authentication.
`priv`	Encryption.
<community-name>	The SNMPv1 or SNMPv2c community name.
<user-name>	SNMPv3 user name.

Mode Global Configuration

Examples To configure the device to send generated traps to the IPv4 host destination `192.0.2.5` with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host  version 2c public192.0.2.5
```

To configure the device to send generated traps to the IPv6 host destination `2001:db8::8a2e:7334` with the SNMPv2c community name private, use the following command:

```
awplus# configure terminal
awplus(config)# snmp-server host  version 2c
private2001:db8::8a2e:7334
```

To remove a configured trap host of 192.0.2.5 with the SNMPv2c community name public, use the following command:

```
awplus# configure terminal
awplus(config)# no snmp-server host  version 2c public192.0.2.5
```

Related Commands

snmp trap link-status

snmp-server enable trap

snmp-server view

snmp-server legacy-ifadminstatus

Overview Use this command to set the ifAdminStatus to reflect the operational state of the interface, rather than the administrative state.

The **no** variant of this command sets the ifAdminStatus to reflect the administrative state of the interface.

Syntax

```
snmp-server legacy-ifadminstatus
no snmp-server legacy-ifadminstatus
```

Default Legacy ifAdminStatus is turned off by default, so by default the SNMP ifAdminStatus reflects the administrative state of the interface.

Mode Global Configuration

Usage Note that if you enable Legacy ifAdminStatus, the ifAdminStatus will report a link's status as Down when the link has been blocked by a process such as loop protection.

Example To turn on Legacy ifAdminStatus, use the command:

```
awplus#snmp-server legacy-ifadminstatus
```

Related Commands show interface

snmp-server location

Overview This command sets the location of the system. The location is:

- displayed in the output of the show system command
- stored in the MIB object sysLocation

The **no** variant of this command removes the configured location from the system.

Syntax

```
snmp-server location <location-name>
no snmp-server location
```

Parameter	Description
<location-name>	The location of the system, from 0 to 255 characters long. Valid characters are any printable character and spaces.

Mode Global Configuration

Example To set the location to “server room 523”, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server location server room 523
```

Related Commands

show snmp-server

show system

snmp-server contact

snmp-server source-interface

Overview Use this command to specify the originating interface for SNMP traps or informs. An interface specified by this command must already have an IP address assigned to it.

Use the **no** variant of this command to reset the interface to its default value (the originating egress interface).

Syntax

```
snmp-server source-interface {traps|informs} <interface-name>
no snmp-server source-interface {traps|informs}
```

Parameter	Description
`traps`	SNMP traps.
`informs`	SNMP informs.
`<interface-name>`	Interface name (must already have an IP address assigned).

Default By default, the source interface is the originating egress interface of the traps and informs messages.

Mode Global Configuration

Usage An SNMP trap or inform message that is sent from an SNMP server carries the notification IP address of its originating interface. Use this command to assign this interface.

Example The following commands set VLAN20 to be the interface whose IP address is used as the originating address in SNMP informs packets.

```
awplus# configure terminal
awplus(config)# snmp-server source-interface informs vlan20
```

The following commands reset the originating source interface for SNMP trap messages to be the default interface (the originating egress interface):

```
awplus# configure terminal
awplus(config)# no snmp-server source-interface traps
```

Validation Commands show running-config

snmp-server startup-trap-delay

Overview Use this command to set the time in seconds after following completion of the device startup sequence before the device sends any SNMP traps (or SNMP notifications).

Use the no variant of this command to restore the default startup delay of 30 seconds.

Syntax

```
snmp-server startup-trap-delay <delay-time>
no snmp-server startup-trap-delay
```

Parameter	Description
<delay-time>	Specify an SNMP trap delay time in seconds in the range of 30 to 600 seconds.

Default The SNMP server trap delay time is 30 seconds. The no variant restores the default.

Mode Global Configuration

Example To delay the device sending SNMP traps until 60 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# snmp-server startup-trap-delay 60
```

To restore the sending of SNMP traps to the default of 30 seconds after device startup, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server startup-trap-delay
```

Validation Commands show snmp-server

snmp-server user

Overview Use this command to create or move users as members of specified groups. This command is used with SNMPv3 only.

The **no** variant of this command removes an SNMPv3 user. The specified user must already exist.

Syntax

```
snmp-server user <username> <groupname> [encrypted] [auth
{md5|sha} <auth-password>] [priv {des|aes} <privacy-password>]
```

```
no snmp-server user <username>
```

Parameter	Description
<username>	User name. The user name is a string up to 20 characters long and is case sensitive.
<groupname>	Group name. The group name is a string up to 20 characters long and is case sensitive.
`encrypted`	Use the encrypted parameter when you want to enter encrypted passwords.
`auth`	Authentication protocol.
`md5`	MD5 Message Digest Algorithms.
`sha`	SHA Secure Hash Algorithm.
<auth-password>	Authentication password. The password is a string of 8 to 20 characters long and is case sensitive.
`priv`	Privacy protocol.
`des`	DES Data Encryption Standard.
`aes`	AES Advanced Encryption Standards.
<privacy-password>	Privacy password. The password is a string of 8 to 20 characters long and is case sensitive.

Mode Global Configuration

Usage Additionally this command provides the option of selecting an authentication protocol and (where appropriate) an associated password. Similarly, options are offered for selecting a privacy protocol and password.

- Note that each SNMP user must be configured on both the manager and agent entities. Where passwords are used, these passwords must be the same for both entities.
- Use the **encrypted** parameter when you want to enter already encrypted passwords in encrypted form as displayed in the running and startup configs stored on the device. For example, you may need to move a user from one group to another group and keep the same passwords for the user instead of removing the user to apply new passwords.

- User passwords are entered using plaintext without the **encrypted** parameter and are encrypted according to the authentication and privacy protocols selected.
- User passwords are viewed as encrypted passwords in running and startup configs shown from **show running-config** and **show startup-config** commands respectively. Copy and paste encrypted passwords from running-configs or startup-configs to avoid entry errors.

Examples To add SNMP user `authuser` as a member of group `usergroup`, with authentication protocol `md5`, authentication password `Authpass`, privacy protocol `des` and privacy password `Privpass`, use the following commands

```
awplus# configure terminal
awplus(config)# snmp-server user authuser usergroup auth md5
Authpass priv des Privpass
```

Validate the user is assigned to the group using the **show snmp-server user** command:

```
awplus#show snmp-server user
Name                Group name          Auth         Privacy
-------             -------------       -------      ----------
authuser            usergroup           md5          des
```

To enter existing SNMP user `authuser` with existing passwords as a member of group `newusergroup` with authentication protocol `md5` plus the encrypted authentication password 0x1c74b9c22118291b0ce0cd883f8dab6b74, privacy protocol `des` plus the encrypted privacy password 0x0e0133db5453ebd03822b004eeacb6608f, use the following commands

```
awplus# configure terminal
awplus(config)# snmp-server user authuser newusergroup
encrypted auth md5 0x1c74b9c22118291b0ce0cd883f8dab6b74 priv
des 0x0e0133db5453ebd03822b004eeacb6608f
```

NOTE: *Copy and paste the encrypted passwords from the **running-config** or the **startup-config** displayed, using the **show running-config** and **show startup- config** commands respectively, into the command line to avoid key stroke errors issuing this command.*

Validate the user has been moved from the first group using the **show snmp-server user** command:

```
awplus#show snmp-server user
Name                Group name          Auth         Privacy
-------             -------------       -------      ----------
authuser            newusergroup        md5          des
```

To delete SNMP user `authuser`, use the following commands:

```
awplus# configure terminal
awplus(config)# no snmp-server user authuser
```

Related Commands

show snmp-server user

snmp-server view

snmp-server view

Overview Use this command to create an SNMP view that specifies a sub-tree of the MIB. Further sub-trees can then be added by specifying a new OID to an existing view. Views can be used in SNMP communities or groups to control the remote manager's access.

NOTE: *The object identifier must be specified in a sequence of integers separated by decimal points.*

The **no** variant of this command removes the specified view on the device. The view must already exist.

Syntax

```
snmp-server view <view-name> <mib-name> {included|excluded}
no snmp-server view <view-name>
```

Parameter	Description
<view-name>	SNMP server view name. The view name is a string up to 20 characters long and is case sensitive.
<mib-name>	Object identifier of the MIB.
`included`	Include this OID in the view.
`excluded`	Exclude this OID in the view.

Mode Global Configuration

Examples The following command creates a view called "loc" that includes the system location MIB sub-tree.

```
awplus(config)# snmp-server view loc 1.3.6.1.2.1.1.6.0 included
```

To remove the view "loc" use the following command

```
awplus(config)# no snmp-server view loc
```

Related Commands

show snmp-server view

snmp-server community

undebug snmp

Overview This command applies the functionality of the no debug snmp command.

45 LLDP Commands

Introduction

Overview

LLDP and LLDP-MED can be configured using the commands in this chapter, or by using SNMP with the LLDP-MIB and LLDP-EXT-DOT1-MIB (see the Support for Allied Telesis Enterprise MIBs in AlliedWare Plus).

The Voice VLAN feature can be configured using commands in VLAN Commands chapter.

For more information about LLDP, see the LLDP Feature Overview and Configuration Guide.

LLDP can transmit a lot of data about the network. Typically, the network information gathered using LLDP is transferred to a Network Management System by SNMP. For security reasons, we recommend using SNMPv3 for this purpose (see the SNMP Feature Overview and Configuration Guide).

LLDP operates over physical ports only. For example, it can be configured on switch ports that belong to static or dynamic channel groups, but not on the channel groups themselves.

Command List

clear lldp statistics

Overview This command clears all LLDP statistics (packet and event counters) associated with specified ports. If no port list is supplied, LLDP statistics for all ports are cleared.

Syntax

```
clear lldp statistics [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the statistics are to be cleared.

Mode Privileged Exec

Examples To clear the LLDP statistics on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp statistics interface port1.0.1,port1.0.6
```

To clear all LLDP statistics for all ports, use the command:

```
awplus# clear lldp statistics
```

Related Commands

show lldp statistics

show lldp statistics interface

clear lldp table

Overview This command clears the table of LLDP information received from neighbors through specified ports. If no port list is supplied, neighbor information is cleared for all ports.

Syntax

```
clear lldp table [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the neighbor information table is to be cleared.

Mode Privileged Exec

Examples To clear the table of neighbor information received on ports 1.0.1 and 1.0.6, use the command:

```
awplus# clear lldp table interface port1.0.1,port1.0.6
```

To clear the entire table of neighbor information received through all ports, use the command:

```
awplus# clear lldp table
```

Related Commands show lldp neighbors

debug lldp

Overview This command enables specific LLDP debug for specified ports. When LLDP debugging is enabled, diagnostic messages are entered into the system log. If no port list is supplied, the specified debugging is enabled for all ports.

The **no** variant of this command disables specific LLDP debug for specified ports. If no port list is supplied, the specified debugging is disabled for all ports.

Syntax

```
debug lldp {[rx][rxpkt][tx][txpkt]} [interface [<port-list>]]
debug lldp operation
no debug lldp {[rx][rxpkt][tx][txpkt]} [interface
[<port-list>]]
no debug lldp operation
no debug lldp all
```

Parameter	Description
`rx`	LLDP receive debug.
`rxpkt`	Raw LLDPDUs received in hex format.
`tx`	LLDP transmit debug.
`txpkt`	Raw Tx LLDPDUs transmitted in hex format.
<port-list>	The ports for which debug is to be configured.
`operation`	Debug for LLDP internal operation on the switch.
`all`	Disables all LLDP debugging for all ports.

Default By default no debug is enabled for any ports.

Mode Privileged Exec

Examples To enable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# debug lldp rx interface port1.0.1,port1.0.6
```

To enable debugging of LLDP transmit with packet dump on all ports, use the command:

```
awplus# debug lldp tx txpkt
```

To disable debugging of LLDP receive on ports 1.0.1 and 1.0.6, use the command:

```
awplus# no debug lldp rx interface port1.0.1,port1.0.6
```

To turn off all LLDP debugging on all ports, use the command:

```
awplus# no debug lldp all
```

Related Commands

show debugging lldp

show running-config lldp

terminal monitor

lldp faststart-count

Overview Use this command to set the fast start count for LLDP-MED. The fast start count determines how many fast start advertisements LLDP sends from a port when it starts sending LLDP-MED advertisements from the port, for instance, when it detects a new LLDP-MED capable device.

The **no** variant of this command resets the LLDPD-MED fast start count to the default (3).

Syntax

```
lldp faststart-count <1-10>
no lldp faststart-count
```

Parameter	Description
<1-10>	The number of fast start advertisements to send.

Default The default fast start count is 3.

Mode Global Configuration

Examples To set the fast start count to 5, use the command:

```
awplus# configure terminal
awplus(config)# lldp faststart-count 5
```

To reset the fast start count to the default setting (3), use the command:

```
awplus# configure terminal
awplus(config)# no lldp faststart-count
```

Related Commands show lldp

lldp holdtime-multiplier

Overview This command sets the holdtime multiplier value. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.

The **no** variant of this command sets the multiplier back to its default.

Syntax

```
lldp holdtime-multiplier <2-10>
no lldp holdtime-multiplier
```

Parameter	Description
<2-10>	The multiplier factor.

Default The default holdtime multiplier value is 4.

Mode Global Configuration

Usage The Time-To-Live defines the period for which the information advertised to the neighbor is valid. If the Time-To-Live expires before the neighbor receives another update of the information, then the neighbor discards the information from its database.

Examples To set the holdtime multiplier to 2, use the commands:

```
awplus# configure terminal
awplus(config)# lldp holdtime-multiplier 2
```

To set the holdtime multiplier back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp holdtime-multiplier 2
```

Related Commands show lldp

lldp management-address

Overview This command sets the IPv4 address to be advertised to neighbors (in the Management Address TLV) via the specified ports. This address will override the default address for these ports.

The **no** variant of this command clears the user-configured management IP address advertised to neighbors via the specified ports. The advertised address reverts to the default.

Syntax

```
lldp management-address <ipaddr>
no lldp management-address
```

Parameter	Description
<ipaddr>	The IPv4 address to be advertised to neighbors, in dotted decimal format. This must be one of the IP addresses already configured on the device.

Default The local loopback interface primary IPv4 address if set, else the primary IPv4 interface address of the lowest numbered VLAN the port belongs to, else the MAC address of the device's baseboard if no VLAN IP addresses are configured for the port.

Mode Interface Configuration

Usage To see the management address that will be advertised, use the show lldp interface command or show lldp local-info command.

Examples To set the management address advertised by ports 1.0.1 and 1.06, to be 192.168.1.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp management-address 192.168.1.6
```

To clear the user-configured management address advertised by ports 1.0.1 and 1.0.6, and revert to using the default address, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp management-address
```

Related Commands show lldp interface

show lldp local-info

lldp med-notifications

Overview Use this command to enable LLDP to send LLDP-MED Topology Change Detected SNMP notifications relating to the specified ports. The switch sends an SNMP event notification when a new LLDP-MED compliant IP Telephony device is connected to or disconnected from a port on the switch.

Use the **no** variant of this command to disable the sending of LLDP-MED Topology Change Detected notifications relating to the specified ports.

Syntax

```
lldp med-notifications
no lldp med-notifications
```

Default The sending of LLDP-MED notifications is disabled by default.

Mode Interface Configuration

Examples To enable the sending of LLDP-MED Topology Change Detected notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-notifications
```

To disable the sending of LLDP-MED notifications relating to ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-notifications
```

Related Commands

lldp notification-interval

lldp notifications

snmp-server enable trap

show lldp interface

lldp med-tlv-select

Overview Use this command to enable LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via the specified ports. The LLDP-MED Capabilities TLV must be enabled before any of the other LLDP-MED Organizationally Specific TLVs are enabled.

Use the **no** variant of this command to disable the specified LLDP-MED Organizationally Specific TLVs for transmission in LLDP advertisements via these ports. In order to disable the LLDP-MED Capabilities TLV, you must also disable the rest of these TLVs. Disabling all these TLVs disables LLDP-MED advertisements.

Syntax

```
lldp med-tlv-select {[capabilities] [network-policy] [location]
[power-management-ext] [inventory-management]}

lldp med-tlv-select all

no lldp med-tlv-select {[capabilities] [network-policy]
[location] [power-management-ext] [inventory-management]}

no lldp med-tlv-select all
```

Parameter	Description
`capabilities`	LLDP-MED Capabilities TLV. When this is enabled, the MAC/PHY Configuration/Status TLV from IEEE 802.3 Organizationally Specific TLVs is also automatically included in LLDP-MED advertisements, whether or not it has been explicitly enabled by the lldp tlv-select command.
`network-policy`	Network Policy TLV. This TLV is transmitted if Voice VLAN parameters have been configured using the commands:
`location`	Location Identification TLV. This TLV is transmitted if location information has been configured using the commands:
`power-management-ext`	Extended Power-via-MDI TLV. This TLV is transmitted if the port is PoE capable, and PoE is enabled (power-inline enable command).
`inventory-management`	Inventory Management TLV Set, including the following TLVs: • Hardware Revision • Firmware Revision • Software Revision • Serial Number • Manufacturer Name • Model Name • Asset ID
`all`	All LLDP-MED Organizationally Specific TLVs.

Default By default LLDP-MED Capabilities, Network Policy, Location Identification and Extended Power-via-MDI TLVs are enabled. Therefore, if LLDP is enabled using the lldp run command, by default LLDP-MED advertisements are transmitted on ports that detect LLDP-MED neighbors connected to them.

Mode Interface Configuration

Usage LLDP-MED TLVs are only sent in advertisements via a port if there is an LLDP-MED-capable device connected to it. To see whether there are LLDP-MED capable devices connected to the ports, use the show lldp neighbors command.

Examples To enable inclusion of the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp med-tlv-select inventory-management
```

To exclude the Inventory TLV Set in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select inventory-management
```

To disable LLDP-MED advertisements transmitted via ports 1.0.1 and 1.0.6, disable all these TLVs using the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp med-tlv-select all
```

Related Commands

lldp tlv-select

location elin-location-id

location civic-location identifier

location civic-location configuration

location coord-location identifier

location coord-location configuration

location elin-location

show lldp interface

switchport voice dscp

switchport voice vlan

switchport voice vlan priority

lldp non-strict-med-tlv-order-check

Overview Use this command to enable non-strict order checking for LLDP-MED advertisements it receives. That is, use this command to enable LLDP to receive and store TLVs from LLDP-MED advertisements even if they do not use standard TLV order.

Use the **no** variant of this command to disable non-strict order checking for LLDP-MED advertisements, that is, to set strict TLV order checking, so that LLDP discards any LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement.

Syntax

```
lldp non-strict-med-tlv-order-check
no lldp non-strict-med-tlv-order-check
```

Default By default TLV non-strict order checking for LLDP-MED advertisements is disabled. That is, strict order checking is applied to LLDP-MED advertisements, according to ANSI/TIA-1057, and LLDP-MED TLVs in non-standard order are discarded.

Mode Global Configuration

Usage The ANSI/TIA-1057 specifies standard order for TLVs in LLDP-MED advertisements, and specifies that if LLDP receives LLDP advertisements with non-standard LLDP-MED TLV order, the TLVs in non-standard order should be discarded. This implementation of LLDP-MED follows the standard: it transmits TLVs in the standard order, and by default discards LLDP-MED TLVs that occur before the LLDP-MED Capabilities TLV in an advertisement. However, some implementations of LLDP transmit LLDP-MED advertisements with non-standard TLV order. To receive and store the data from these non-standard advertisements, enable non-strict order checking for LLDP-MED advertisements using this command.

Examples To enable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tlv-order-check
```

To disable strict TLV order checking, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tlv-order-check
```

Related Commands show running-config lldp

lldp notification-interval

Overview This command sets the notification interval. This is the minimum interval between LLDP SNMP notifications (traps) of each kind (LLDP Remote Tables Change Notification and LLDP-MED Topology Change Notification).

The **no** variant of this command sets the notification interval back to its default.

Syntax

```
lldp notification-interval <5-3600>
no lldp notification-interval
```

Parameter	Description
<5-3600>	The interval in seconds.

Default The default notification interval is 5 seconds.

Mode Global Configuration

Examples To set the notification interval to 20 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp notification-interval 20
```

To set the notification interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp notification-interval
```

Related Commands lldp notifications

show lldp

lldp notifications

Overview This command enables the sending of LLDP SNMP notifications (traps) relating to specified ports.

The **no** variant of this command disables the sending of LLDP SNMP notifications for specified ports.

Syntax

```
lldp notifications
no lldp notifications
```

Default The sending of LLDP SNMP notifications is disabled by default.

Mode Interface Configuration

Examples To enable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp notifications
```

To disable sending of LLDP SNMP notifications for ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp notifications
```

Related Commands

lldp notification-interval

show lldp interface

snmp-server enable trap

lldp port-number-type

Overview This command sets the type of port identifier used to enumerate, that is to count, the LLDP MIB local port entries. The LLDP MIB (IEEE Standard 802.1AB-2005, Section 12, LLDP MIB Definitions.) requires the port number value to count LLDP local port entries.

This command also enables you to optionally set an interface index to enumerate the LLDP MIB local port entries, if required by your management system.

The **no** variant of this command resets the type of port identifier back to the default setting (number).

Syntax

```
lldp port-number-type [number|ifindex]
no lldp port-number-type
```

Parameter	Description
`number`	Set the type of port identifier to a port number to enumerate the LLDP MIB local port entries.
`ifindex`	Set the type of port identifier to an interface index to enumerate the LLDP MIB local port entries.

Default The default port identifier type is number. The no variant of this command sets the port identifier type to the default.

Mode Global Configuration

Examples To set the type of port identifier used to enumerate LLDP MIB local port entries to port numbers, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type number
```

To set the type of port identifier used to enumerate LLDP MIB local port entries to interface indexes, use the commands:

```
awplus# configure terminal
awplus(config)# lldp port-number-type ifindex
```

To reset the type of port identifier used to enumerate LLDP MIB local port entries the default (port numbers), use the commands:

```
awplus# configure terminal
awplus(config)# no lldp port-number-type
```

Related Commands show lldp

lldp reinit

Overview This command sets the value of the reinitialization delay. This is the minimum time after disabling LLDP on a port before it can reinitialize.

The **no** variant of this command sets the reinitialization delay back to its default setting.

Syntax

```
lldp reinit <1-10>
no lldp reinit
```

Parameter	Description
<1-10>	The delay in seconds.

Default The default reinitialization delay is 2 seconds.

Mode Global Configuration

Examples To set the reinitialization delay to 3 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp reinit 3
```

To set the reinitialization delay back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp reinit
```

Related Commands show lldp

lldp run

Overview This command enables the operation of LLDP on the device.

The **no** variant of this command disables the operation of LLDP on the device. The LLDP configuration remains unchanged.

Syntax

```
lldp run
no lldp run
```

Default LLDP is disabled by default.

Mode Global Configuration

Examples To enable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# lldp run
```

To disable LLDP operation, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp run
```

Related Commands show lldp

lldp timer

Overview This command sets the value of the transmit interval. This is the interval between regular transmissions of LLDP advertisements.

The **no** variant of this command sets the transmit interval back to its default.

Syntax

```
lldp timer <5-32768>
no lldp timer
```

Parameter	Description
<5-32768>	The transmit interval in seconds. The transmit interval must be at least four times the transmission delay timer (lldp tx-delay command).

Default The default transmit interval is 30 seconds.

Mode Global Configuration

Examples To set the transmit interval to 90 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp timer 90
```

To set the transmit interval back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp timer
```

Related Commands lldp tx-delay

show lldp

lldp tlv-select

Overview This command enables one or more optional TLVs, or all TLVs, for transmission in LLDP advertisements via the specified ports. The TLVs can be specified in any order; they are placed in LLDP frames in a fixed order (as described in IEEE 802.1AB). The mandatory TLVs (Chassis ID, Port ID, Time To Live, End of LLDPDU) are always included in LLDP advertisements.

In LLDP-MED advertisements the MAC/PHY Configuration/Status TLV will be always be included regardless of whether it is selected by this command.

The **no** variant of this command disables the specified optional TLVs, or all optional TLVs, for transmission in LLDP advertisements via the specified ports.

Syntax

```
lldp tlv-select {[<tlv>]...}
lldp tlv-select all
no lldp tlv-select {[<tlv>]...}
no lldp tlv-select all
```

Parameter	Description
`<tlv>`	The TLV to transmit in LLDP advertisements. One of these keywords: • port-description (specified by the description (interface) command) • system-name (specified by the hostname command) • system-description • system-capabilities • management-address • port-vlan • port-and-protocol-vlans • vlan-names • protocol-ids • mac-phy-config • power-management (Power Via MDI TLV) • link-aggregation • max-frame-size
`all`	All TLVs.

Default By default no optional TLVs are included in LLDP advertisements. The MAC/PHY Configuration/Status TLV (**mac-phy-config**) is included in LLDP-MED advertisements whether or not it is selected by this command.

Mode Interface Configuration

Examples

To include the management-address and system-name TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select management-address
system-name
```

To include all optional TLVs in advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp tlv-select all
```

To exclude the management-address and system-name TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select management-address
system-name
```

To exclude all optional TLVs from advertisements transmitted via ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp tlv-select all
```

Related Commands

description (interface)

hostname

lldp med-tlv-select

show lldp interface

show lldp local-info

lldp transmit receive

Overview This command enables transmission and/or reception of LLDP advertisements to or from neighbors through the specified ports.

The **no** variant of this command disables transmission and/or reception of LLDP advertisements through specified ports.

Syntax

```
lldp {[transmit] [receive]}
no lldp {[transmit] [receive]}
```

Parameter	Description
`transmit`	Enable or disable transmission of LLDP advertisements via this port or ports.
`receive`	Enable or disable reception of LLDP advertisements via this port or ports.

Default LLDP advertisement transmission and reception are enabled on all ports by default.

Mode Interface Configuration

Examples To enable transmission of LLDP advertisements on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit
```

To enable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# lldp transmit receive
```

To disable LLDP advertisement transmission and reception on ports 1.0.1 and 1.0.6, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.6
awplus(config-if)# no lldp transmit receive
```

Related Commands show lldp interface

lldp tx-delay

Overview This command sets the value of the transmission delay timer. This is the minimum time interval between transmitting LLDP advertisements due to a change in LLDP local information.

The **no** variant of this command sets the transmission delay timer back to its default setting.

Syntax

```
lldp tx-delay <1-8192>
no lldp tx-delay
```

Parameter	Description
<1-8192>	The transmission delay in seconds. The transmission delay cannot be greater than a quarter of the transmit interval (lldp timer command).

Default The default transmission delay timer is 2 seconds.

Mode Global Configuration

Examples To set the transmission delay timer to 12 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# lldp tx-delay 12
```

To set the transmission delay timer back to its default, use the commands:

```
awplus# configure terminal
awplus(config)# no lldp tx-delay
```

Related Commands lldp timer

show lldp

location civic-location configuration

Overview Use these commands to configure a civic address location. The country parameter must be specified first, and at least one of the other parameters must be configured before the location can be assigned to a port.

Use the **no** variants of this command to delete civic address parameters from the location.

Syntax

```
country <country>
state <state>
no state
county <county>
no county
city <city>
no city
division <division>
no division
neighborhood <neighborhood>
no neighborhood
street-group <street-group>
no street-group
leading-street-direction <leading-street-direction>
no leading-street-direction
trailing-street-suffix <trailing-street-suffix>
no trailing-street-suffix
street-suffix <street-suffix>
no street-suffix
house-number <house-number>
no house-number
house-number-suffix <house-number-suffix>
no house-number-suffix
landmark <landmark>
no landmark
additional-information <additional-information>
no additional-information
```

Syntax (cont.)

```
name <name>
no name
postalcode <postalcode>
no postalcode
building <building>
no building
unit <unit>
no unit
floor <floor>
no floor
room <room>
no room
place-type <place-type>
no place-type
postal-community-name <postal-community-name>
no postal-community-name
post-office-box <post-office-box>
no post-office-box
additional-code <additional-code>
no additional-code
seat <seat>
no seat
primary-road-name <primary-road-name>
no primary-road-name
road-section <road-section>
no road-section
branch-road-name <branch-road-name>
no branch-road-name
sub-branch-road-name <sub-branch-road-name>
no sub-branch-road-name
street-name-pre-modifier <street-name-pre-modifier>
no street-name-pre-modifier
streetname-post-modifier <streetname-post-modifier>
no streetname-post-modifier
```

Parameter	Description
<country>	Upper-case two-letter country code, as specified in ISO 3166.
<state>	State (Civic Address (CA) Type 1): national subdivisions (state, canton, region).
<county>	County (CA Type 2): County, parish, gun (JP), district (IN).
<city>	City (CA Type 3): city, township, shi (JP).
<division>	City division (CA Type 4): City division, borough, city district, ward, chou (JP).
<neighborhood>	Neighborhood (CA Type 5): neighborhood, block.
<street-group>	Street group (CA Type 6): group of streets below the neighborhood level.
<leading-street-direction>	Leading street direction (CA Type 16).
<trailing-street-suffix>	Trailing street suffix (CA Type 17).
<street-suffix>	Street suffix (CA Type 18): street suffix or type.
<house-number>	House number (CA Type 19).
<house-number-suffix>	House number suffix (CA Type 20).
<landmark>	Landmark or vanity address (CA Type 21).
<additional-information>	Additional location information (CA Type 22).
<name>	Name (CA Type 23): residence and office occupant.
<postal-code>	Postal/zip code (CA Type 24).
<building>	Building (CA Type 25): structure.
<unit>	Unit (CA Type 26): apartment, suite.
<floor>	Floor (CA Type 27).
<room>	Room (CA Type 28).
<place-type>	Type of place (CA Type 29).
<postal-community-name>	Postal community name (CA Type 30).
<post-office-box>	Post office box (P.O. Box) (CA Type 31).
<additional-code>	Additional code (CA Type 32).
<seat>	Seat (CA Type 33): seat (desk, cubicle, workstation).
<primary-road-name>	Primary road name (CA Type 34).
<road-section>	Road section (CA Type 35).

Parameter	Description
<branch-road-name>	Branch road name (CA Type 36).
<sub-branch-road-name>	Sub-branch road name (CA Type 37).
<street-name-pre-modifier>	Street name pre-modifier (CA Type 38).
<street-name-post-modifier>	Street name post-modifier (CA Type 39).

Default By default no civic address location information is configured.

Mode Civic Address Location Configuration

Usage The **country** parameter must be configured before any other parameters can be configured; this creates the location. The country parameter cannot be deleted. One or more of the other parameters must be configured before the location can be assigned to a port. The country parameter must be entered as an upper-case two-letter country code, as specified in ISO 3166. All other parameters are entered as alpha-numeric strings. Do not configure all the civic address parameters (this would generate TLVs that are too long). Configure a subset of these parameters—enough to consistently and precisely identify the location of the device. If the location is to be used for Emergency Call Service (ECS), the particular ECS application may have guidelines for configuring the civic address location. For more information about civic address format, see the LLDP Feature Overview and Configuration Guide.

To specify the civic address location, use the location civic-location identifier command. To delete the civic address location, use the **no** variant of the **location civic-location identifier** command. To assign the civic address location to particular ports, so that it can be advertised in TLVs from those ports, use the command location civic-location-id command.

Examples To configure civic address location 1 with location "27 Nazareth Avenue, Christchurch, New Zealand" in civic-address format, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)# country NZ
awplus(config-civic)# city Christchurch
awplus(config-civic)# primary-road-name Nazareth
awplus(config-civic)# street-suffix Avenue
awplus(config-civic)# house-number 27
```

Related Commands location civic-location-id

location civic-location identifier

show lldp local-info

show location

location civic-location identifier

Overview Use this command to enter the Civic Address Location Configuration mode to configure the specified location.

Use the **no** variant of this command to delete a civic address location. This also removes the location from any ports it has been assigned to.

Syntax

```
location civic-location identifier <civic-loc-id>
no location civic-location identifier <civic-loc-id>
```

Parameter	Description
<civic-loc-id>	A unique civic address location ID, in the range 1 to 4095.

Default By default there are no civic address locations.

Mode Global Configuration

Usage To configure the location information for this civic address location identifier, use the location civic-location configuration command. To associate this civic location identifier with particular ports, use the location elin-location-id command.

Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

Examples To enter Civic Address Location Configuration mode for the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location civic-location identifier 1
awplus(config-civic)#
```

To delete the civic address location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location civic-location identifier 1
```

Related Commands

location civic-location-id

location civic-location configuration

show location

show running-config lldp

location civic-location-id

Overview Use this command to assign a civic address location to the ports. The civic address location must already exist. This replaces any previous assignment of civic address location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

Syntax

```
location civic-location-id <civic-loc-id>
no location civic-location-id [<civic-loc-id>]
```

Parameter	Description
<civic-loc-id>	Civic address location ID, in the range 1 to 4095.

Default By default no civic address location is assigned to ports.

Mode Interface Configuration

Usage The civic address location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, create the location using the following commands:

- location civic-location identifier command
- location civic-location configuration command

If a civic-address location is deleted using the **no** variant of the location civic-location identifier command, it is automatically removed from all ports.

Examples To assign the civic address location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location civic-location-id 1
```

To remove a civic address location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location civic-location-id
```

Related Commands

lldp med-tlv-select

location civic-location identifier

location civic-location configuration

show location

location coord-location configuration

Overview Use this command to configure a coordinate-based location. All parameters must be configured before assigning this location identifier to a port.

Syntax

```
latitude <latitude>
lat-resolution <lat-resolution>
longitude <longitude>
long-resolution <long-resolution>
altitude <altitude> {meters|floor}
alt-resolution <alt-resolution>
datum {wgs84|nad83-navd|nad83-mllw}
```

Parameter	Description
<lat-resolution>	Latitude resolution, as a number of valid bits, in the range 0 to 34.
<latitude>	Latitude value in degrees in the range -90.0 to 90.0
<long-resolution>	Longitude resolution, as a number of valid bits, in the range 0 to 34.
<longitude>	Longitude value in degrees, in the range -180.0 to 180.0.
<alt-resolution>	Altitude resolution, as a number of valid bits, in the range 0 to 30. A resolution of 0 can be used to indicate an unknown value.
<altitude>	Altitude value, in meters or floors.
`meters`	The altitude value is in meters.
`floors`	The altitude value is in floors.
`datum`	The geodetic system (or datum) that the specified coordinate values are based on.
`wgs84`	World Geodetic System 1984.
`nad83-navd`	North American Datum 1983 - North American Vertical Datum.
`nad83-mllw`	North American Datum 1983 - Mean Lower Low Water vertical datum.

Default By default no coordinate location information is configured.

Mode Coordinate Configuration

Usage Latitude and longitude values are always stored internally, and advertised in the Location Identification TLV, as 34-bit fixed-point binary numbers, with a 25-bit fractional part, irrespective of the number of digits entered by the user. Likewise

altitude is stored as a 30- bit fixed point binary number, with an 8-bit fractional part. Because the user-entered decimal values are stored as fixed point binary numbers, they cannot always be represented exactly—the stored binary number is converted to a decimal number for display in the output of the show location command. For example, a user-entered latitude value of "2.77" degrees is displayed as "2.76999998092651367187500000".

The **lat-resolution**, **long-resolution**, and **alt-resolution** parameters allow the user to specify the resolution of each coordinate element as the number of valid bits in the internally-stored binary representation of the value. These resolution values can be used by emergency services to define a search area.

To specify the coordinate identifier, use the location coord-location identifier command. To remove coordinate information, delete the coordinate location by using the **no** variant of that command. To associate the coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the location elin-location-id command.

Example To configure the location for the White House in Washington DC, which has the coordinates based on the WGS84 datum of 38.89868 degrees North (with 22 bit resolution), 77.03723 degrees West (with 22 bit resolution), and 15 meters height (with 9 bit resolution), use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)# la-resolution 22
awplus(config-coord)# latitude 38.89868
awplus(config-coord)# lo-resolution 22
awplus(config-coord)# longitude -77.03723
awplus(config-coord)# alt-resolution 9
awplus(config-coord)# altitude 15 meters
awplus(config-coord)# datum wgs84
```

Related Commands

location coord-location-id

location coord-location identifier

show lldp local-info

show location

location coord-location identifier

Overview Use this command to enter Coordinate Location Configuration mode for this coordinate location.

Use the **no** variant of this command to delete a coordinate location. This also removes the location from any ports it has been assigned to.

Syntax

```
location coord-location identifier <coord-loc-id>
no location coord-location identifier <coord-loc-id>
```

Parameter	Description
<coord-loc-id>	A unique coordinate location identifier, in the range 1 to 4095.

Default By default there are no coordinate locations.

Mode Global Configuration

Usage Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To configure this coordinate location, use the location coord-location configuration command. To associate this coordinate location with particular ports, so that it can be advertised in TLVs from those ports, use the location coord-location-id command.

Examples To enter Coordinate Location Configuration mode to configure the coordinate location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# location coord-location identifier 1
awplus(config-coord)#
```

To delete coordinate location 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location coord-location identifier 1
```

Related Commands

location coord-location-id

location coord-location configuration

show lldp local-info

show location

location coord-location-id

Overview Use this command to assign a coordinate location to the ports. The coordinate location must already exist. This replaces any previous assignment of coordinate location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location from the ports.

Syntax

```
location coord-location-id <coord-loc-id>
no location coord-location-id [<coord-loc-id>]
```

Parameter	Description
<coord-loc-id>	Coordinate location ID, in the range 1 to 4095.

Default By default no coordinate location is assigned to ports.

Mode Interface Configuration

Usage The coordinate location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the following commands:

- location coord-location identifier command
- location coord-location configuration command

If a coordinate location is deleted using the **no** variant of the location coord-location identifier command, it is automatically removed from all ports.

Examples To assign coordinate location 1 to port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location coord-location-id 1
```

To remove a coordinate location from port1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location coord-location-id
```

Related Commands

lldp med-tlv-select

location coord-location identifier

location coord-location configuration

show location

location elin-location

Overview Use this command to create or modify an ELIN location.

Use the **no** variant of this command to delete an ELIN location, and remove it from any ports it has been assigned to.

Syntax

```
location elin-location <elin> identifier <elin-loc-id>
no location elin-location identifier <elin-loc-id>
```

Parameter	Description
<elin>	Emergency Location Identification Number (ELIN) for Emergency Call Service (ECS), in the range 10 to 25 digits long. In North America, ELINs are typically 10 digits long.
<elin-loc-id>	A unique ELIN location identifier, in the range 1 to 4095.

Default By default there are no ELIN location identifiers.

Mode Global Configuration

Usage Up to 400 locations can be configured on the switch for each type of location information, up to a total of 1200 locations.

To assign this ELIN location to particular ports, so that it can be advertised in TLVs from those ports, use the location elin-location-id command.

Examples To create a new ELIN location with ID 1, and configure it with ELIN "1234567890", use the commands:

```
awplus# configure terminal
awplus(config)# location elin-location 1234567890 identifier 1
```

To delete existing ELIN location with ID 1, use the commands:

```
awplus# configure terminal
awplus(config)# no location elin-location identifier 1
```

Related Commands

location elin-location-id

show lldp local-info

show location

location elin-location-id

Overview Use this command to assign an ELIN location to the ports. The ELIN location must already exist. This replaces any previous assignment of ELIN location for the ports. Up to one location of each type can be assigned to a port.

Use the **no** variant of this command to remove a location identifier from the ports.

Syntax

```
location elin-location-id <elin-loc-id>
no location elin-location-id [<elin-loc-id>]
```

Parameter	Description
<elin-loc-id>	ELIN location identifier, in the range 1 to 4095.

Default By default no ELIN location is assigned to ports.

Mode Interface Configuration

Usage An ELIN location associated with a port can be transmitted in Location Identification TLVs via the port.

Before using this command, configure the location using the location elin-location command.

If an ELIN location is deleted using the **no** variant of one of the location elin-location command, it is automatically removed from all ports.

Examples To assign ELIN location 1 to port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# location elin-location-id 1
```

To remove an ELIN location from port 1.0.1, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1
awplus(config-if)# no location elin-location-id
```

Related Commands

lldp med-tlv-select

location elin-location

show location

show debugging lldp

Overview This command displays LLDP debug settings for specified ports. If no port list is supplied, LLDP debug settings for all ports are displayed.

Syntax

```
show debugging lldp [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the LLDP debug settings are shown.

Mode User Exec and Privileged Exec

Examples To display LLDP debug settings for all ports, use the command:

```
awplus# show debugging lldp
```

To display LLDP debug settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show debugging lldp interface port1.0.1-1.0.6
```

Output Figure 45-1: Example output from the **show debugging lldp** command

```
LLDP Debug settings:
Debugging for LLDP internal operation is on
Port       Rx    RxPkt   Tx    TxPkt
-----------------------------------
1.0.1      Yes   Yes     No    No
1.0.2      Yes   No      No    No
1.0.3      No    No      No    No
1.0.4      Yes   Yes     Yes   No
1.0.5      Yes   No      Yes   No
1.0.6      Yes   Yes     Yes   Yes
```

Table 1: Parameters in the output of the **show debugging lldp** command

Parameter	Description
Port	Port name.
Rx	Whether debugging of LLDP receive is enabled on the port.
RxPkt	Whether debugging of LLDP receive packet dump is enabled on the port.
Rx	Whether debugging of LLDP transmit is enabled on the port.
RxPkt	Whether debugging of LLDP transmit packet dump is enabled on the port.

Related Commands debug lldp

show lldp

Overview This command displays LLDP status and global configuration settings.

Syntax

```
show lldp
```

Mode User Exec and Privileged Exec

Example To display LLDP status and global configuration settings, use the command:

```
awplus# show lldp
```

Output

Table 2: Example output from the **show lldp** command

```
awplus# show lldp

LLDP Global Configuration:              [Default Values]
LLDP Status ............... Enabled     [Disabled]
Notification Interval ..... 5 secs      [5]
Tx Timer Interval ......... 30 secs     [30]
Hold-time Multiplier ...... 4           [4]
(Computed TTL value ....... 120 secs)
Reinitialization Delay .... 2 secs      [2]
Tx Delay .................. 2 secs      [2]

Port Number Type........... Ifindex     [Port-Number]
Fast Start Count .......... 5           [3]

LLDP Global Status:
Total Neighbor Count ...... 47
Neighbors table last updated 0 hrs 0 mins 43 secs ago
```

Table 3: Parameters in the output of the **show lldp** command

Parameter	Description
LLDP Status	Whether LLDP is enabled. Default is disabled.
Notification Interval	Minimum interval between LLDP notifications.
Tx Timer Interval	Transmit interval between regular transmissions of LLDP advertisements.
Hold-time Multiplier	The holdtime multiplier. The transmit interval is multiplied by the holdtime multiplier to give the Time To Live (TTL) value that is advertised to neighbors.
Reinitialization Delay	The reinitialization delay. This is the minimum time after disabling LLDP transmit on a port before it can reinitialize again.

Table 3: Parameters in the output of the **show lldp** command (cont.)

Parameter	Description
`Tx Delay`	The transmission delay. This is the minimum time interval between transmitting advertisements due to a change in LLDP local information.
`Port Number Type`	The type of port identifier used to enumerate LLDP MIB local port entries, as set by the lldp port-number-type command.
`Fast Start Count`	The number of times fast start advertisements are sent for LLDP-MED.
`Total Neighbor Count`	Number of LLDP neighbors discovered on all ports.
`Neighbors table last updated`	The time since the LLDP neighbor table was last updated.

Related Commands

show lldp interface

show running-config lldp

show lldp interface

Overview This command displays LLDP configuration settings for specified ports. If no port list is specified, LLDP configuration for all ports is displayed.

Syntax

```
show lldp interface [<port-list>]
```

Parameter	Description
<port-list>	The ports for which the LLDP configuration settings are to be shown.

Mode User Exec and Privileged Exec

Examples To display LLDP configuration settings for ports 1.0.1 to 1.0.6, use the command:

```
awplus# show lldp interface port1.0.1-1.0.6
```

To display LLDP configuration settings for all ports, use the command:

```
awplus# show lldp interface
```

Output Figure 45-2: Example output from the **show lldp interface** command

```
awplus# show lldp interface port1.0.1-1.0.8
LLDP Port Status and Configuration:

  * = LLDP is inactive on this port because it is a mirror analyser port
  Notification Abbreviations:
    RC = LLDP Remote Tables Change       TC = LLDP-MED Topology Change
  TLV Abbreviations:
    Base:  Pd = Port Description         Sn = System Name
           Sd = System Description       Sc = System Capabilities
           Ma = Management Address
    802.1: Pv = Port VLAN ID             Pp = Port And Protocol VLAN ID
           Vn = VLAN Name                Pi = Protocol Identity
    802.3: Mp = MAC/PHY Config/Status    Po = Power Via MDI (PoE)
           La = Link Aggregation         Mf = Maximum Frame Size
    MED:   Mc = LLDP-MED Capabilities    Np = Network Policy
           Lo = Location Identification  Pe = Extended PoE    In = Inventory

                                          Optional TLVs Enabled for Tx
 Port     Rx/Tx  Notif  Management Addr  Base       802.1    802.3    MED
-------------------------------------------------------------------------------
 1.0.1    Rx Tx  RC --  192.168.100.123  PdSnSdScMa -------- -------- McNpLoPe--
*1.0.2    -- Tx  RC --  192.168.100.123  PdSnSdScMa -------- -------- McNpLoPe--
 1.0.3    Rx Tx  RC --  192.168.100.123  Pd--SdScMa PvPpVnPi -------- McNpLoPe--
 1.0.4    -- --  RC --  192.168.100.123  PdSnSd--Ma -------- -------- McNpLoPe--
 1.0.5    Rx Tx  RC TC  192.168.100.123  PdSnSdScMa PvPpVnPi -------- McNpLoPe--
 1.0.6    Rx Tx  RC TC  192.168.100.123  Pd----ScMa -------- -------- McNpLoPe--
 1.0.7    Rx Tx  -- TC  192.168.100.123  PdSnSdScMa PvPpVnPi MpPoLaMf McNpLoPeIn
 1.0.8    Rx Tx  -- TC  192.168.1.1      PdSn--ScMa PvPpVnPi -------- McNp------
```

Table 4: Parameters in the output of the **show lldp interface** command

Parameter	Description
`Port`	Port name.
`Rx`	Whether reception of LLDP advertisements is enabled on the port.
`Tx`	Whether transmission of LLDP advertisements is enabled on the port.
`Notif`	Whether sending SNMP notification for LLDP is enabled on the port: • RM = Remote Tables Change Notification • TP = LLDP-MED Topology Change Notification
`Management Addr`	Management address advertised to neighbors.
`Base TLVs Enabled for Tx`	List of optional Base TLVs enabled for transmission: • Pd = Port Description • Sn =System Name • Sd = System Description • Sc =System Capabilities • Ma = Management Address
`802.1 TLVs Enabled for Tx`	List of optional 802.1 TLVs enabled for transmission: • Pv = Port VLAN ID • Pp = Port And Protocol VLAN ID • Vn = VLAN Name • Pi =Protocol Identity
`802.3 TLVs Enabled for Tx`	List of optional 802.3 TLVs enabled for transmission: • Mp = MAC/PHY Configuration/Status • Po = Power Via MDI (PoE) • La = Link Aggregation • Mf = Maximum Frame Size
`MED TLVs Enabled for Tx`	List of optional LLDP-MED TLVs enabled for transmission: • Mc = LLDP-MED Capabilities • Np = Network Policy • Lo = Location Information, • Pe = Extended Power-Via-MDI • In = Inventory

Related Commands

show lldp

show running-config lldp

show lldp local-info

Overview This command displays local LLDP information that can be transmitted through specified ports. If no port list is entered, local LLDP information for all ports is displayed.

Syntax

```
show lldp local-info [base] [dot1] [dot3] [med] [interface
<port-list>]
```

Parameter	Description
`base`	Information for base TLVs.
`dot1`	Information for 802.1 TLVs.
`dot3`	Information for 802.3 TLVs.
`med`	Information for LLDP-MED TLVs.
<port-list>	The ports for which the local information is to be shown.

Mode User Exec and Privileged Exec

Usage Whether and which local information is transmitted in advertisements via a port depends on:

- whether the port is set to transmit LLDP advertisements (lldp transmit receive command)
- which TLVs it is configured to send (lldp tlv-select command, lldp med-tlv-select command)

Examples To display local information transmitted via port 1.0.1, use the command:

```
awplus# show lldp local-info interface port1.0.1
```

To display local information transmitted via all ports, use the command:

```
awplus# show lldp local-info
```

Output Figure 45-3: Example output from **show lldp local-info**

```
LLDP Local Information:

Local port1.1.1:
  Chassis ID Type ................... MAC address
  Chassis ID ........................ 0015.77c9.7453
  Port ID Type ...................... Interface alias
  Port ID ........................... port1.0.1
  TTL ............................... 120
  Port Description .................. [not configured]
```

```
System Name ..................... awplus
System Description .............. Allied Telesis router/switch, AW+
                                  v5.4.5
System Capabilities - Supported .. Bridge, Router
                    - Enabled .... Bridge, Router
Management Address .............. 192.168.1.6
Port VLAN ID (PVID) ............. 1
Port & Protocol VLAN - Supported . Yes
                     - Enabled ... No
                     - VIDs ..... 0
VLAN Names ...................... default
Protocol IDs .................... 9000, 0026424203000000, 888e01, aaaa03,
                                  88090101, 00540000e302, 0800, 0806, 86dd
MAC/PHY Auto-negotiation ........ Supported, Enabled
     Advertised Capability ...... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                  10BaseTFD, 10BaseT
     Operational MAU Type ....... 1000BaseTFD (30)
Power Via MDI (PoE) ............. Supported, Enabled
     Port Class ................. PSE
     Pair Control Ability ....... Disabled
     Power Class ................ Unknown
Link Aggregation ................ Supported, Disabled
Maximum Frame Size .............. 1522
LLDP-MED Device Type ............ Network Connectivity
LLDP-MED Capabilities ........... LLDP-MED Capabilities, Network Policy,
                                  Location Identification,
                                  Extended Power - PSE, Inventory
Network Policy .................. [not configured]
Location Identification ......... Civic Address
     Country Code ............... NZ
     City ....................... Christchurch
     Street Suffix .............. Avenue
     House Number ............... 27
     Primary Road Name .......... Nazareth
Location Identification ......... ELIN
     ELIN ....................... 123456789012
LLDP-MED Device Type ............ Network Connectivity
LLDP-MED Capabilities ........... LLDP-MED Capabilities, Network Policy,
                                  Location Identification,
                                  Extended Power - PSE, Inventory
Extended Power Via MDI (PoE) ..... PSE
     Power Source ............... Primary Power
     Power Priority ............. Low
     Power Value ................ 4.4 Watts
Inventory Management:
     Hardware Revision .......... A-0
     Firmware Revision .......... 1.1.0
     Software Revision .......... v5.4.5
     Serial Number .............. G1Q78900B
     Manufacturer Name .......... Allied Telesis Inc.
     Model Name ................. x610-48Ts/XP
     Asset ID ................... [zero length]
```

Table 45-1: Parameters in the output of **show lldp local-info**

Parameter	Description
`Chassis ID Type`	Type of the Chassis ID.
`Chassis ID`	Chassis ID that uniquely identifies the local device.
`Port ID Type`	Type of the Port ID.
`Port ID`	Port ID of the local port through which advertisements are sent.
`TTL`	Number of seconds that the information advertised by the local port remains valid.
`Port Description`	Port description of the local port, as specified by the description (interface) command.
`System Name`	System name, as specified by the hostname command.
`System Description`	System description.
`System Capabilities (Supported)`	Capabilities that the local port supports.
`System Capabilities (Enabled)`	Enabled capabilities on the local port.
`Management Addresses`	Management address associated with the local port. To change this, use the lldp management-address command.
`Port VLAN ID (PVID)`	VLAN identifier associated with untagged or priority tagged frames received via the local port.
`Port & Protocol VLAN (Supported)`	Whether Port & Protocol VLANs (PPV) is supported on the local port.
`Port & Protocol VLAN (Enabled)`	Whether the port is in one or more Port & Protocol VLANs.
`Port & Protocol VLAN (VIDs)`	List of identifiers for Port & Protocol VLANs that the port is in.
`VLAN Names`	List of VLAN names for VLANs that the local port is assigned to.
`Protocol IDs`	List of protocols that are accessible through the local port.
`MAC/PHY Auto-negotiation`	Auto-negotiation support and current status of the 802.3 LAN on the local port.

Table 45-1: Parameters in the output of **show lldp local-info** (cont.)

Parameter	Description
Power Via MDI (PoE)	PoE-capability and current status on the local port.
Port Class	Whether the device is a PSE (Power Sourcing Entity) or a PD (Powered Device)
Pair Control Ability	Whether power pair selection can be controlled
Power Pairs	Which power pairs are selected for power ("Signal Pairs" or "Spare Pairs") if pair selection can be controlled
Power Class	The power class of the PD device on the port (class 0, 1, 2, 3 or 4)
Link Aggregation	Whether the link is capable of being aggregated and it is currently in an aggregation.
Aggregated Port-ID	Aggregated port identifier.
Maximum Frame Size	The maximum frame size capability of the implemented MAC and PHY.
LLDP-MED Device Type	LLDP-MED device type
LLDP-MED Capabilities	Capabilities LLDP-MED capabilities supported on the local port.
Network Policy	List of network policies configured on the local port.
VLAN ID	VLAN identifier for the port for the specified application type
Tagged Flag	Whether the VLAN ID is to be used as tagged or untagged
Layer-2 Priority:	Layer 2 User Priority (in the range 0 to 7)
DSCP Value	Diffserv codepoint (in the range 0 to 63)
Location Identification	Location configured on the local port.
Extended Power Via MDI (PoE)	PoE-capability and current status of the PoE parameters for Extended Power-Via-MDI TLV on the local port.
Power Source	The power source the switch currently uses; either primary power or backup power.
Power Priority	The power priority configured on the port; either critical, high or low.

Table 45-1: Parameters in the output of **show lldp local-info** (cont.)

Parameter	Description
`Power Value`	The total power the switch can source over a maximum length cable to a PD device on the port. The value shows the power value in Watts from the PD side.
`Inventory Management`	Inventory information for the device.

Related Commands

description (interface)

hostname

lldp transmit receive

show lldp neighbors

Overview This command displays a summary of information received from neighbors via specified ports. If no port list is supplied, neighbor information for all ports is displayed.

Syntax

```
show lldp neighbors [interface <port-list>]
```

Parameter	Description
<port-list>	The ports for which the neighbor information is to be shown.

Mode User Exec and Privileged Exec

Examples To display neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors
```

To display neighbor information received via ports 1.0.1 and 1.0.6 with LLDP-MED configuration, use the command:

```
awplus# show lldp neighbors interface port1.0.1,port1.0.6
```

Output Figure 45-4: Example output from the **show lldp neighbors** command

```
LLDP Neighbor Information:

Total number of neighbors on these ports .... 4

  System Capability Codes:
    O = Other    P = Repeater   B = Bridge                W = WLAN Access Point
    R = Router   T = Telephone  C = DOCSIS Cable Device   S = Station Only
  LLDP-MED Device Type and Power Source Codes:
    1 = Class I    3 = Class III    PSE  = PoE    Both = PoE&Local   Prim = Primary
    2 = Class II   N = Network Con. Locl = Local  Unkn = Unknown     Back = Backup

Local    Neighbor        Neighbor        Neighbor                System      MED
Port     Chassis ID      Port ID         Sys Name                Cap.        Ty Pwr
-------------------------------------------------------------------------------
1.0.1    002d.3044.7ba6  port1.0.2       awplus                  OPBWRTCS
1.0.1    0011.3109.e5c6  port1.0.3       AT-9924 switch/route... --B-R---
1.0.6    0000.10cf.8590  port3           AR-442S                 --B-R---
1.0.6    00ee.4352.df51  192.168.1.2     Jim's desk phone        --B--T--    3  PSE
```

Table 46: Parameters in the output of the **show lldp neighbors** command

Parameter	Description
`Local Port`	Local port on which the neighbor information was received.
`Neighbor Chassis ID`	Chassis ID that uniquely identifies the neighbor.
`Neighbor Port Name`	Port ID of the neighbor.
`Neighbor Sys Name`	System name of the LLDP neighbor.
`Neighbor Capability`	Capabilities that are supported and enabled on the neighbor.
`System Capability`	System Capabilities of the LLDP neighbor.
`MED Device Type`	LLDP-MED Device class (Class I, II, III or Network Connectivity)
`MED Power Source`	LLDP-MED Power Source

Related Commands show lldp neighbors detail

show lldp neighbors detail

Overview This command displays in detail the information received from neighbors via specified ports. If no port list is supplied, detailed neighbor information for all ports is displayed.

Syntax

```
show lldp neighbors detail [base] [dot1] [dot3] [med] [interface
<port-list>]
```

Parameter	Description
`base`	Information for base TLVs.
`dot1`	Information for 802.1 TLVs.
`dot3`	Information for 803.1 TLVs.
`med`	Information for LLDP-MED TLVs.
<port-list>	The ports for which the neighbor information is to be shown.

Mode User Exec and Privileged Exec

Examples To display detailed neighbor information received via all ports, use the command:

```
awplus# show lldp neighbors detail
```

To display detailed neighbor information received via ports 1.0.1, use the command:

```
awplus# show lldp neighbors detail interface port1.0.1
```

Output Figure 45-5: Example output from the **show lldp neighbors detail** command

```
awplus# show lldp neighbors detail interface port1.0.1
LLDP Detailed Neighbor Information:

Local port1.0.1:
  Neighbors table last updated 0 hrs 0 mins 40 secs ago

  Chassis ID Type ................... MAC address
  Chassis ID ........................ 0004.cd28.8754
  Port ID Type ...................... Interface alias
  Port ID ........................... port1.0.6
  TTL ............................... 120 (secs)
  Port Description .................. [zero length]
  System Name ....................... awplus
  System Description ................ Allied Telesis router/switch, AW+ v5.4.4
  System Capabilities - Supported .. Bridge, Router
                      - Enabled .... Bridge, Router
  Management Addresses .............. 0004.cd28.8754
  Port VLAN ID (PVID) ............... 1
  Port & Protocol VLAN - Supported . Yes
                       - Enabled ... Yes
                       - VIDs ...... 5
  VLAN Names ........................ default, vlan5
  Protocol IDs ...................... 9000, 0026424203000000, 888e01, 8100,
                                      88090101, 00540000e302, 0800, 0806, 86dd
  MAC/PHY Auto-negotiation ......... Supported, Enabled
       Advertised Capability ....... 1000BaseTFD, 100BaseTXFD, 100BaseTX,
                                      10BaseTFD, 10BaseT
       Operational MAU Type ........ 1000BaseTFD (30)
  Power Via MDI (PoE) ............... [not advertised]
  Link Aggregation .................. Supported, Disabled
  Maximum Frame Size ................ 1522 (Octets)
  LLDP-MED Device Type .............. Network Connectivity
  LLDP-MED Capabilities ............. LLDP-MED Capabilities, Network Policy,
                                      Location Identification,
                                      Extended Power - PSE, Inventory
  Network Policy .................... [not advertised]
  Location Identification ........... [not advertised]
  Extended Power Via MDI (PoE) ..... PD
           Power Source ............. PSE
           Power Priority ........... High
           Power Value .............. 4.4 Watts
  Inventory Management:
           Hardware Revision ........ X1-0
           Firmware Revision ........ 1.1.0
           Software Revision ........ v5.4.4
           Serial Number ............ M1NB73008
           Manufacturer Name ........ Allied Telesis Inc.
           Model Name ............... SBx908
           Asset ID ................. [zero length]
```

Table 47: Parameters in the output of the **show lldp neighbors detail** command

Parameter	Description
`Chassis ID Type`	Type of the Chassis ID.
`Chassis ID`	Chassis ID that uniquely identifies the neighbor.
`Port ID Type`	Type of the Port ID.
`Port ID`	Port ID of the neighbor.
`TTL`	Number of seconds that the information advertised by the neighbor remains valid.
`Port Description`	Port description of the neighbor's port.
`System Name`	Neighbor's system name.
`System Description`	Neighbor's system description.
`System Capabilities (Supported)`	Capabilities that the neighbor supports.
`System Capabilities (Enabled)`	Capabilities that are enabled on the neighbor.
`Management Addresses`	List of neighbor's management addresses.
`Port VLAN ID (PVID)`	VLAN identifier associated with untagged or priority tagged frames for the neighbor port.
`Port & Protocol VLAN (Supported)`	Whether Port & Protocol VLAN is supported on the LLDP neighbor.
`Port & Protocol VLAN (Enabled)`	Whether Port & Protocol VLAN is enabled on the LLDP neighbor.
`Port & Protocol VLAN (VIDs)`	List of Port & Protocol VLAN identifiers.
`VLAN Names`	List of names of VLANs that the neighbor's port belongs to.
`Protocol IDs`	List of protocols that are accessible through the neighbor's port.
`MAC/PHY Auto-negotiation`	Auto-negotiation configuration and status
`Power Via MDI (PoE)`	PoE configuration and status of 802.3 Power-Via-MDI TLV
`Link Aggregation`	Link aggregation information

Table 47: Parameters in the output of the **show lldp neighbors detail** command (cont.)

Parameter	Description
`Maximum Frame Size`	The maximum frame size capability
`LLDP-MED Device Type`	LLDP-MED Device type
`LLDP-MED Capabilities`	LLDP-MED capabilities supported
`Network Policy`	List of network policies
`Location Identification`	Location information
`Extended Power Via MDI (PoE)`	PoE-capability and current status
`Inventory Management`	Inventory information

Related Commands show lldp neighbors

show lldp statistics

Overview This command displays the global LLDP statistics (packet and event counters).

Syntax

```
show lldp statistics
```

Mode User Exec and Privileged Exec

Example To display global LLDP statistics information, use the command:

```
awplus# show lldp statistics
```

Output

Table 48: Example output from the **show lldp statistics** command

```
awplus# show lldp statistics

Global LLDP Packet and Event counters:

  Frames:    Out ................... 345
             In .................... 423
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 20
             Deleted Entries ....... 20
             Dropped Entries ....... 0
             Entry Age-outs ........ 20
```

Table 49: Parameters in the output of the **show lldp statistics** command

Parameter	Description
Frames Out	Number of LLDPDU frames transmitted.
Frames In	Number of LLDPDU frames received.
Frames In Errored	Number of invalid LLDPDU frames received.
Frames In Dropped	Number of LLDPDU frames received and discarded for any reason.
TLVs Unrecognized	Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.
TLVs Discarded	Number of LLDP TLVs discarded for any reason.
Neighbors New Entries	Number of times the information advertised by neighbors has been inserted into the neighbor table.

Table 49: Parameters in the output of the **show lldp statistics** command (cont.)

Parameter	Description
`Neighbors Deleted Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table.
`Neighbors Dropped Entries`	Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
`Neighbors Entry Age-outs Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

Related Commands

clear lldp statistics

show lldp statistics interface

show lldp statistics interface

Overview This command displays the LLDP statistics (packet and event counters) for specified ports. If no port list is supplied, LLDP statistics for all ports are displayed.

Syntax

```
show lldp statistics interface [<port-list>]
```

Parameter	Description
<port-list>	The ports for which the statistics are to be shown.

Mode User Exec and Privileged Exec

Examples To display LLDP statistics information for all ports, use the command:

```
awplus# show lldp statistics interface
```

To display LLDP statistics information for ports 1.0.1 and 1.0.6, use the command:

```
awplus# show lldp statistics interface port1.0.1,port1.0.6
```

Output

Table 50: Example output from the **show lldp statistics interface** command

```
awplus# show lldp statistics interface port1.0.1,port1.0.6

LLDP Packet and Event Counters:

port1.0.1
  Frames:    Out ................... 27
             In .................... 22
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 3
             Deleted Entries ....... 0
             Dropped Entries ....... 0
             Entry Age-outs ........ 0

port1.0.6
  Frames:    Out ................... 15
             In .................... 18
             In Errored ............ 0
             In Dropped ............ 0
  TLVs:      Unrecognized .......... 0
             Discarded ............. 0
  Neighbors: New Entries ........... 1
             Deleted Entries ....... 0
             Dropped Entries ....... 0
             Entry Age-outs ........ 0
```

Table 51: Parameters in the output of the **show lldp statistics interface** command

Parameter	Description
`Frames Out`	Number of LLDPDU frames transmitted.
`Frames In`	Number of LLDPDU frames received.
`Frames In Errored`	Number of invalid LLDPDU frames received.
`Frames In Dropped`	Number of LLDPDU frames received and discarded for any reason.
`TLVs Unrecognized`	Number of LLDP TLVs received that are not recognized but the TLV type is in the range of reserved TLV types.
`TLVs Discarded`	Number of LLDP TLVs discarded for any reason.
`Neighbors New Entries`	Number of times the information advertised by neighbors has been inserted into the neighbor table.
`Neighbors Deleted Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table.
`Neighbors Dropped Entries`	Number of times the information advertised by neighbors could not be entered into the neighbor table because of insufficient resources.
`Neighbors Entry Age-outs Entries`	Number of times the information advertised by neighbors has been removed from the neighbor table because the information TTL interval has expired.

Related Commands

clear lldp statistics

show lldp statistics

show location

Overview Use this command to display selected location information configured on the switch.

Syntax

```
show location {civic-location|coord-location|elin-location}
show location {civic-location|coord-location|elin-location}
identifier {<civic-loc-id>|<coord-loc-id>|<elin-loc-id>}
show location {civic-location|coord-location|elin-location}
interface <port-list>
```

Parameter	Description
`civic-location`	Display civic location information.
`coord-location`	Display coordinate location information.
`elin-location`	Display ELIN location information.
<civic-loc-id>	Civic address location identifier, in the range 1 to 4095.
<coord-loc-id>	Coordinate location identifier, in the range 1 to 4095.
<elin-loc-id>	ELIN location identifier, in the range 1 to 4095.
<port-list>	Ports to display information about.

Mode User Exec and Privileged Exec

Examples To display a civic address location configured on port1.0.1, use the command:

```
awplus# show location civic-location interface port1.0.1
```

Table 52: Example output from the **show location** command

```
awplus# show location civic-location interface port1.0.1
Port     ID   Element Type          Element Value
-------------------------------------------------------------
1.0.1    1    Country               NZ
              City                  Christchurch
              Street-suffix         Avenue
              House-number          27
              Primary-road-name     Nazareth
```

To display coordinate location information configured on the identifier 1, use the command:

```
awplus# show location coord-location identifier 1
```

Table 53: Example output from the **show location** command

```
awplus# show location coord-location identifier 1
  ID  Element Type             Element Value
------------------------------------------------------------------
  1   Latitude Resolution      15 bits
      Latitude                 38.898648113012313842773437 5 degrees
      Longitude Resolution     15 bits
      Longitude                130.232322293128967285156250 degrees
      Altitude Resolution      10 bits
      Altitude                 2.50000000 meters
      Map Datum                WGS 84
```

The coordinate location information displayed may differ from the information entered because it is stored in binary format. For more information, see the location coord-location configuration command.

To display all ELIN location information configured on the switch, use the command:

```
awplus# show location elin-location
```

Table 54: Example output from the **show location elin-location** command

```
awplus# show location elin-location
  ID  ELIN
-----------------------------------
  1   1234567890
  2   5432154321
```

Related Commands

location elin-location-id

location civic-location identifier

location civic-location configuration

location coord-location identifier

location coord-location configuration

location elin-location

46 SMTP Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure SMTP.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

debug mail

Overview This command turns on debugging for sending emails.

The **no** variant of this command turns off debugging for sending emails.

Syntax

```
debug mail
no debug mail
```

Mode Privileged Exec

Examples To turn on debugging for sending emails, use the command:

```
awplus# debug mail
```

To turn off debugging for sending emails, use the command:

```
awplus# no debug mail
```

Related Commands

delete mail

mail

mail from

mail smtpserver

show mail

show counter mail

undebug mail

delete mail

Overview This command deletes mail from the queue.

Syntax

```
delete mail [mail-id <mail-id>|all]
```

Parameter	Description	
`mail-id`	Deletes a single mail from the mail queue.	
	`<mail-id>`	An unique mail ID number. Use the show mail command to display this for an item of mail.
`all`	Delete all the mail in the queue.	

Mode Privileged Exec

Examples To delete a unique mail item `20060912142356.1234` from the queue, use the command:

```
awplus# delete mail 20060912142356.1234
```

To delete all mail from the queue, use the command:

```
awplus# delete mail all
```

Related Commands

debug mail

mail

mail from

mail smtpserver

show mail

mail

Overview This command sends an email using the SMTP protocol. If you specify a file the text inside the file is sent in the message body.

If you do not specify the **to**, **file**, or **subject** parameters, the CLI prompts you for the missing information.

Before you can send mail using this command, you must specify the sending email address using the mail from command and a mail server using the mail smtpserver command.

Syntax `mail [{to <to>|subject <subject>|file <filename>}]`

Parameter	Description
`to`	The email recipient.
	<to> Email address.
`subject`	Description of the subject of this email. Use quote marks when the subject text contains spaces.
	<subject> String.
`file`	File to insert as text into the message body.
	<filename> String.

Mode Privileged Exec

Example To send an email to `rei@nerv.com`with the subject `dummy plug configuration`, and with the message body inserted from the file `plug.conf` use the command:

```
awplus# mail rei@nerv.com subject dummy plug configuration
filename plug.conf
```

Related Commands

debug mail

delete mail

mail from

mail smtpserver

show mail

show counter mail

mail from

Overview This command sets an email address for the “mail from” SMTP command. You must specify a sending email address with this command before you can send any email.

Syntax

```
mail from <from>
```

Parameter	Description
<from>	The email address that the mail is sent from.

Mode Global Configuration

Example To set the email address from which you are sending mail to “kaji@nerv.com”, use the command:

```
awplus(config)# mail from kaji@nerv.com
```

Related Commands

delete mail

mail

mail smtpserver

show mail

mail smtpserver

Overview This command sets the IP address of the SMTP server that your device sends email to. You must specify a mail server with this command before you can send any email.

Syntax

```
mail smtpserver <ip-address>
```

Parameter	Description
<ip-address>	Internet Protocol (IP) Address for the mail server specified.

Mode Global Configuration

Example To specify a mail server at 192.168.0.1, use the command:

```
awplus# mail smtpserver 192.168.0.1
```

Related Commands

debug mail

delete mail

mail

mail from

show mail

show counter mail

show counter mail

Overview This command displays the mail counters.

Syntax

```
show counter mail
```

Mode User Exec and Privileged Exec

Output Figure 46-1: Example output from the **show counter mail** command

```
Mail Client (SMTP) counters
Mails Sent            ......... 0
Mails Sent Fails      ......... 1
```

Table 1: Parameters in the output of the **show counter mail** command

Parameter	Description
Mails Sent	The number of emails sent successfully since the last device restart.
Mails Sent Fails	The number of emails the device failed to send since the last device restart.

Example To show the emails in the queue use the command:

```
awplus# show counter mail
```

Related Commands

debug mail

delete mail

mail

mail from

show mail

show mail

Overview This command displays the emails in the queue.

Syntax

```
show mail
```

Mode Privileged Exec

Example To display the emails in the queue use the command:

```
awplus# show mail
```

Related Commands

delete mail

mail

show counter mail

undebug mail

Overview This command applies the functionality of the no debug mail command.

47 RMON Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Remote Monitoring (RMON).

For an introduction to RMON and an RMON configuration example, see the RMON Feature Overview and Configuration Guide.

RMON is disabled by default in AlliedWare Plus™. No RMON alarms or events are configured.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

rmon alarm

Overview Use this command to configure an RMON alarm to monitor the value of an SNMP object, and to trigger specified events when the monitored object crosses specified thresholds.

To specify the action taken when the alarm is triggered, use the event index of an event defined by the rmon event command.

Use the **no** variant of this command to remove the alarm configuration.

NOTE: *Only alarms for switch port interfaces, not for VLAN interfaces, can be configured.*

Syntax

```
rmon alarm <alarm-index> <oid> interval <1-2147483647>
{delta|absolute} rising-threshold <1-2147483647> event
<rising-event-index> falling-threshold <1-2147483647> event
<falling-event-index> alarmstartup [1|2|3] [owner <owner>]
```

```
no rmon alarm <alarm-index>
```

Parameter	Description
<alarm-index>	*<1-65535>* Alarm entry index value.
<oid>	The variable SNMP MIB Object Identifier (OID) name to be monitored, in the format etherStatsEntry.*<field>*.*<stats-index>*. For example, etherStatsEntry.5.22 is the OID for the etherStatsPkts field in the etherStatsEntry table for the interface defined by the *<stats-index>* 22 in the rmon collection stats command.
interval *<1-2147483647>*	Polling interval in seconds.
delta	The RMON MIB alarmSampleType: the change in the monitored MIB object value between the beginning and end of the polling interval.
absolute	The RMON MIB alarmSampleType: the value of the monitored MIB object.
rising-threshold *<1-2147483647>*	Rising threshold value of the alarm entry in seconds.
<rising-event-index>	*<1-65535>* The event to be triggered when the monitored object value reaches the rising threshold value. This is an event index of an event specified by the rmon event command.
falling-threshold *<1-2147483647>*	Falling threshold value of the alarm entry in seconds.
<falling-event-index>	*<1-65535>* The event to be triggered when the monitored object value reaches the falling threshold value. This is an event index of an event specified by the rmon event command.

Parameter	Description
`alarmstartup {1|2|3}`	Whether RMON can trigger a falling alarm (1), a rising alarm (2) or either (3) when you first start monitoring. See the Usage section for more information. The default is setting 3 (either).
`owner <owner>`	Arbitrary owner name to identify the alarm entry.

Default By default, there are no alarms.

Mode Global Configuration

Usage RMON alarms have a rising and falling threshold. Once the alarm monitoring is operating, you cannot have a falling alarm unless there has been a rising alarm and vice versa.

However, when you start RMON alarm monitoring, an alarm must be generated without the other type of alarm having first been triggered. The **alarmstartup** parameter allows this. It is used to say whether RMON can generate a rising alarm (1), a falling alarm (2) or either alarm (3) as the first alarm.

Note that the SNMP MIB Object Identifier (OID) indicated in the command syntax with <*oid*> must be specified as a dotted decimal value with the form etherStatsEntry.<*field*>.<*stats-index*>, for example, etherStatsEntry.22.5.

Example To configure an alarm to monitor the change per minute in the etherStatsPkt value for interface 22 (defined by stats-index 22 in the rmon collection stats command), to trigger event 2 (defined by the rmon event command) when it reaches the rising threshold 400, and to trigger event 3 when it reaches the falling threshold 200, and identify this alarm as belonging to Maria, use the commands:

```
awplus# configure terminal
awplus(config)# rmon alarm 229 etherStatsEntry.22.5 interval 60
delta rising-threshold 400 event 2 falling-threshold 200 event
3 alarmstartup 3 owner maria
```

Related Commands rmon collection stats

rmon event

rmon collection history

Overview Use this command to create a history statistics control group to store a specified number of snapshots (buckets) of the standard RMON statistics for the switch port, and to collect these statistics at specified intervals. If there is sufficient memory available, then the device will allocate memory for storing the set of buckets that comprise this history control.

Use the **no** variant of this command to remove the specified history control configuration.

NOTE: *Only a history for switch port interfaces, not for VLAN interfaces, can be collected.*

Syntax

```
rmon collection history <history-index> [buckets <1-65535>]
[interval <1-3600>] [owner <owner>]
```

```
no rmon collection history <history-index>
```

Parameter	Description
<history-index>	*<1-65535>* A unique RMON history control entry index value.
buckets *<1-65535>*	Number of requested buckets to store snapshots. Default 50 buckets.
interval *<1-3600>*	Polling interval in seconds. Default 1800 second polling interval.
owner*<owner>*	Owner name to identify the entry.

Default The default interval is 1800 seconds and the default buckets is 50 buckets.

Mode Interface Configuration

Example To create a history statistics control group to store 200 snapshots with an interval of 500 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection history 200 buckets 500
interval 600 owner herbert
```

To disable the history statistics control group, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection history 200
```

rmon collection stats

Overview Use this command to enable the collection of RMON statistics on a switch port, and assign an index number by which to access these collected statistics.

Use the **no** variant of this command to stop collecting RMON statistics on this switch port.

NOTE: *Only statistics for switch port interfaces, not for VLAN interfaces, can be collected.*

Syntax

```
rmon collection stats <collection-index> [owner <owner>]
no rmon collection stats <collection-index>
```

Parameter	Description
<collection-index>	*<1-65535>* Give this collection of statistics an index number to uniquely identify it. This is the index to use to access the statistics collected for this switch port.
owner *<owner>*	An arbitrary owner name to identify this statistics collection entry.

Default RMON statistics are not enabled by default.

Mode Interface Configuration

Example To enable the collection of RMON statistics with a statistics index of 200, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# rmon collection stats 200 owner myrtle
```

To to stop collecting RMON statistics, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.2
awplus(config-if)# no rmon collection stats 200
```

rmon event

Overview Use this command to create an event definition for a log or a trap or both. The event index for this event can then be referred to by the rmon alarm command.

Use the **no** variant of this command to remove the event definition.

NOTE: *Only the events for switch port interfaces, not for VLAN interfaces, can be collected.*

Syntax

```
rmon event <event-index> [description <description>|owner
<owner>| trap <trap>]
```

```
rmon event <event-index> [log [description <description>|owner
<owner>|trap <trap>] ]
```

```
rmon event <event-index> [log trap [description
<description>|owner <owner] ]
```

```
no rmon event <event-index>
```

Parameter	Description
<event-index>	*<1-65535>* Unique event entry index value.
log	Log event type.
trap	Trap event type.
log trap	Log and trap event type.
description*<description>*	Event entry description.
owner *<owner>*	Owner name to identify the entry.

Default No event is configured by default.

Mode Global Configuration

Example To create an event definition for a log with an index of 299, use this command:

```
awplus# configure terminal
awplus(config)# rmon event 299 log description cond3 owner
alfred
```

To to remove the event definition, use the command:

```
awplus# configure terminal
awplus(config)# no rmon event 299
```

Related Commands rmon alarm

show rmon alarm

Overview Use this command to display the alarms and threshold configured for the RMON probe.

NOTE: *Only the alarms for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon alarm
```

Mode User Exec and Privileged Exec

Example To display the alarms and threshold, use this command:

```
awplus# show rmon alarm
```

Related Commands rmon alarm

show rmon event

Overview Use this command to display the events configured for the RMON probe.

NOTE: *Only the events for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon event
```

Mode User Exec and Privileged Exec

Output Figure 47-1: Example output from the **show rmon event** command

```
awplus#sh rmon event
 event Index = 787
       Description TRAP
        Event type log & trap
         Event community name gopher
       Last Time Sent = 0
       Owner  RMON_SNMP

 event Index = 990
       Description TRAP
        Event type trap
         Event community name teabo
       Last Time Sent = 0
       Owner  RMON_SNMP
```

NOTE: *The following etherStats counters are not currently available for Layer 3 interfaces:*

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets
- etherStatsPkts1024to1518Octets

Example To display the events configured for the RMON probe, use this command:

```
awplus# show rmon event
```

Related Commands rmon event

show rmon history

Overview Use this command to display the parameters specified on all the currently defined RMON history collections on the device.

NOTE: *Only the history for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon history
```

Mode User Exec and Privileged Exec

Output Figure 47-2: Example output from the **show rmon history** command

```
awplus#sh rmon history
 history index = 56
         data source ifindex = 4501
         buckets requested = 34
        buckets granted = 34
        Interval = 2000
        Owner Andrew

 history index = 458
         data source ifindex = 5004
         buckets requested = 400
        buckets granted = 400
        Interval = 1500
        Owner trev
=========================================================
```

NOTE: *The following etherStats counters are not currently available for Layer 3 interfaces:*

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets

- etherStatsPkts1024to1518Octets

Example To display the parameters specified on all the currently defined RMON history collections, us the commands:

```
awplus# show rmon history
```

Related Commands rmon collection history

show rmon statistics

Overview Use this command to display the current values of the statistics for all the RMON statistics collections currently defined on the device.

NOTE: *Only statistics for switch port interfaces, not for VLAN interfaces, can be shown.*

Syntax

```
show rmon statistics
```

Mode User Exec and Privileged Exec

Example To display the current values of the statistics for all the RMON statistics collections, us the commands:

```
awplus# show rmon statistics
```

Output Figure 47-3: Example output from the **show rmon statistics** command

```
awplus#show rmon statistics
    rmon collection index 45
    stats->ifindex = 4501
    input packets 1279340, bytes 85858960, dropped 00, multicast packets 1272100
    output packets 7306090, bytes 268724, multicast packets 7305660 broadcast
packets 290
    rmon collection index 679
    stats->ifindex = 5013
    input packets 00, bytes 00, dropped 00, multicast packets 00
    output packets 8554550, bytes 26777324, multicast packets 8546690 broadcast
packets 7720
```

NOTE: *The following etherStats counters are not currently available for Layer 3 interfaces:*

- etherStatsBroadcastPkts
- etherStatsCRCAlignErrors
- etherStatsUndersizePkts
- etherStatsOversizePkts
- etherStatsFragments
- etherStatsJabbers
- etherStatsCollisions
- etherStatsPkts64Octets
- etherStatsPkts65to127Octets
- etherStatsPkts128to255Octets
- etherStatsPkts256to511Octets
- etherStatsPkts512to1023Octets

- etherStatsPkts1024to1518Octets

Related Commands rmon collection stats

48 Secure Shell (SSH) Commands

Introduction

Overview This chapter provides an alphabetical reference for commands used to configure Secure Shell (SSH). For more information, see the SSH Feature Overview and Configuration Guide.

Command List

banner login (SSH)

Overview This command configures a login banner on the SSH server. This displays a message on the remote terminal of the SSH client before the login prompt. SSH client version 1 does not support this banner.

To add a banner, first enter the command **banner login**, and hit [Enter]. Write your message. You can use any character and spaces. Use Ctrl+D at the end of your message to save the text and re-enter the normal command line mode.

The banner message is preserved if the device restarts.

The **no** variant of this command deletes the login banner from the device.

Syntax

```
banner login
no banner login
```

Default No banner is defined by default.

Mode Global Configuration

Examples To set a login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# banner login
```

The screen will prompt you to enter the message:

```
Type CNTL/D to finish.
... banner message comes here ...
```

Enter the message. Use Ctrl+D to finish, like this:

```
^D
awplus(config)#
```

To remove the login banner message, use the commands:

```
awplus# configure terminal
awplus(config)# no banner login
```

Related Commands show banner login

clear ssh

Overview This command deletes Secure Shell sessions currently active on the device. This includes both incoming and outgoing sessions. The deleted sessions are closed. You can only delete an SSH session if you are a system manager or the user who initiated the session. If **all** is specified then all active SSH sessions are deleted.

Syntax

```
clear ssh {<1-65535>|all}
```

Parameters	Description
<1-65535>	Specify a session ID in the range 1 to 65535 to delete a specific session.
`all`	Delete all SSH sessions.

Mode Privileged Exec

Examples To stop the current SSH session 123, use the command:

```
awplus# clear ssh 123
```

To stop all SSH sessions active on the device, use the command:

```
awplus# clear ssh all
```

Related Commands service ssh

ssh

crypto key destroy hostkey

Overview This command deletes the existing public and private keys of the SSH server. Note that for an SSH server to operate it needs at least one set of hostkeys configured before an SSH server is started.

Syntax

```
crypto key destroy hostkey {dsa|rsa|rsa1}
```

Parameters	Description
`dsa`	Deletes the existing DSA public and private keys.
`rsa`	Deletes the existing RSA public and private keys configured for SSH version 2 connections.
`rsa1`	Deletes the existing RSA public and private keys configured for SSH version 1 connections.

Mode Global Configuration

Example To destroy the RSA host key used for SSH version 2 connections, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy hostkey rsa
```

Related Commands

crypto key generate hostkey

service ssh

crypto key destroy userkey

Overview This command destroys the existing public and private keys of an SSH user configured on the device.

Syntax

```
crypto key destroy userkey <username> {dsa|rsa|rsa1}
```

Parameters	Description
<*username*>	Name of the user whose userkey you are destroying. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Deletes the existing DSA userkey.
rsa	Deletes the existing RSA userkey configured for SSH version 2 connections.
rsa1	Deletes the existing RSA userkey for SSH version 1 connections.

Mode Global Configuration

Example To destroy the RSA user key for the SSH user `remoteuser`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key destroy userkey remoteuser rsa
```

Related Commands

crypto key generate hostkey

show ssh

show crypto key hostkey

crypto key generate hostkey

Overview This command generates public and private keys for the SSH server using either an RSA or DSA cryptography algorithm. You must define a host key before enabling the SSH server. Start SSH server using the **service ssh** command. If a host key exists with the same cryptography algorithm, this command replaces the old host key with the new key.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax

```
crypto key generate hostkey {dsa|rsa|rsa1} [<768-32768>]
```

Parameters	Description
`dsa`	Creates a DSA hostkey. Both SSH version 1 and 2 connections can use the DSA hostkey.
`rsa`	Creates an RSA hostkey for SSH version 2 connections.
`rsa1`	Creates an RSA hostkey for SSH version 1 connections.
<768-32768>	The length in bits of the generated key. The default is 1024 bits.

Default 1024 bits is the default key length. The DSA algorithm supports 1024 bits.

Mode Global Configuration

Examples To generate an RSA host key for SSH version 2 connections that is 2048 bits in length, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 2048
```

To generate a DSA host key, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate dsa
```

Related Commands

crypto key destroy hostkey

service ssh

show crypto key hostkey

crypto key generate userkey

Overview This command generates public and private keys for an SSH user using either an RSA or DSA cryptography algorithm. To use public key authentication, copy the public key of the user onto the remote SSH server.

This command is not saved in the device configuration. However, the device saves the keys generated by this command in the non-volatile memory.

Syntax

```
crypto key generate userkey <username> {dsa|rsa|rsa1}
[<768-32768>]
```

Parameters	Description
<username>	Name of the user that the user key is generated for. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Creates a DSA userkey. Both SSH version 1 and 2 connections can use a key created with this command.
rsa	Creates an RSA userkey for SSH version 2 connections.
rsa1	Creates an RSA userkey for SSH version 1 connections.
<768-32768>	The length in bits of the generated key. The DSA algorithm supports only 1024 bits. Default: 1024.

Mode Global Configuration

Examples To generate a 2048-bits RSA user key for SSH version 2 connections for the user `bob`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey bob rsa 2048
```

To generate a DSA user key for the user `lapo`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key generate userkey lapo dsa
```

Related Commands

crypto key pubkey-chain userkey

show crypto key userkey

crypto key pubkey-chain knownhosts

Overview This command adds a public key of the specified SSH server to the known host database on your device. The SSH client on your device uses this public key to verify the remote SSH server.

The key is retrieved from the server. Before adding a key to this database, check that the key sent to you is correct.

If the server's key changes, or if your SSH client does not have the public key of the remote SSH server, then your SSH client will inform you that the public key of the server is unknown or altered.

The **no** variant of this command deletes the public key of the specified SSH server from the known host database on your device.

Syntax

```
crypto key pubkey-chain knownhosts [ip|ipv6] <hostname>
[rsa|dsa|rsa1]
no crypto key pubkey-chain knownhosts <1-65535>
```

Parameter	Description
`ip`	Keyword used prior to specifying an IPv4 address
`ipv6`	Keyword used prior to specifying an IPv6 address
<hostname>	IPv4/IPv6 address or hostname of a remote server in the format `a.b.c.d` for an IPv4 address, or in the format `x:x::x:x` for an IPv6 address.
`rsa`	Specify the RSA public key of the server to be added to the known host database.
`dsa`	Specify the DSA public key of the server to be added to the known host database.
`rsa1`	Specify the SSHv1 public key of the server to be added to the know host database.
<1-65535>	Specify a key identifier when removing a key using the **no** parameter.

Default If no cryptography algorithm is specified, then **rsa** is used as the default cryptography algorithm.

Mode Privilege Exec

Usage This command adds a public key of the specified SSH server to the known host database on the device. The key is retrieved from the server. The remote SSH server is verified by using this public key. The user is requested to check the key is correct before adding it to the database.

If the remote server's host key is changed, or if the device does not have the public key of the remote server, then SSH clients will inform the user that the public key of the server is altered or unknown.

Examples

To add the RSA host key of the remote SSH host IPv4 address `192.0.2.11` to the known host database, use the command:

```
awplus# crypto key pubkey-chain knownhosts 192.0.2.11
```

To delete the second entry in the known host database, use the command:

```
awplus# no crypto key pubkey-chain knownhosts 2
```

Validation Commands

show crypto key pubkey-chain knownhosts

crypto key pubkey-chain userkey

Overview This command adds a public key for an SSH user on the SSH server. This allows the SSH server to support public key authentication for the SSH user. When configured, the SSH user can access the SSH server without providing a password from the remote host.

The **no** variant of this command removes a public key for the specified SSH user that has been added to the public key chain. When a SSH user's public key is removed, the SSH user can no longer login using public key authentication.

Syntax

```
crypto key pubkey-chain userkey <username> [<filename>]
no crypto key pubkey-chain userkey <username> <1-65535>
```

Parameters	Description
<username>	Name of the user that the SSH server associates the key with. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols. Default: no default
<filename>	Filename of a key saved in flash. Valid characters are any printable character. You can add a key as a hexadecimal string directly into the terminal if you do not specify a filename.
<1-65535>	The key ID number of the user's key. Specify the key ID to delete a key.

Mode Global Configuration

Usage You should import the public key file from the client node. The device can read the data from a file on the flash or user terminal.

Or you can add a key as text into the terminal. To add a key as text into the terminal, first enter the command **crypto key pubkey-chain userkey** <*username*>, and hit [Enter]. Enter the key as text. Note that the key you enter as text must be a valid SSH RSA key, not random ASCII text. Use [Ctrl]+D after entering it to save the text and re-enter the normal command line mode.

Note you can generate a valid SSH RSA key on the device first using the **crypto key generate host rsa** command. View the SSH RSA key generated on the device using the **show crypto hostkey rsa** command. Copy and paste the displayed SSH RSA key after entering the **crypto key pubkey-chain userkey** <*username*> command. Use [Ctrl]+D after entering it to save it.

Examples To generate a valid SSH RSA key on the device and add the key, use the following commands:

```
awplus# configure terminal
awplus(config)# crypto key generate host rsa
awplus(config)# exit
awplus# show crypto key hostkey
rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20bWluh
nUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4UxOKSD
tTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4SvfZZfe
ITzvvyZW4/I4pbN8=
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey joeType CNTL/D
to
finish:AAAAB3NzaC1yc2EAAAABIwAAAIEAr1s7SokW5aW2fcOw1TStpb9J20b
WluhnUC768EoWhyPW6FZ2t5360O5M29EpKBmGqlkQaz5V0mU9IQe66+5YyD4Ux
OKSDtTI+7jtjDcoGWHb2u4sFwRpXwJZcgYrXW16+6NvNbk+h+c/pqGDijj4Svf
ZZfeITzvvyZW4/I4pbN8=control-D
awplus(config)#
```

To add a public key for the user `graydon` from the file `key.pub`, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey graydon key.pub
```

To add a public key for the user `tamara` from the terminal, use the commands:

```
awplus# configure terminal
awplus(config)# crypto key pubkey-chain userkey tamara
```

and enter the key. Use Ctrl+D to finish.

To remove the first key entry from the public key chain of the user `john`, use the commands:

```
awplus# configure terminal
awplus(config)# no crypto key pubkey-chain userkey john 1
```

Related Commands show crypto key pubkey-chain userkey

debug ssh client

Overview This command enables the SSH client debugging facility. When enabled, any SSH, SCP and SFTP client sessions send diagnostic messages to the login terminal.

The **no** variant of this command disables the SSH client debugging facility. This stops the SSH client from generating diagnostic debugging message.

Syntax

```
debug ssh client [brief|full]
no debug ssh client
```

Parameter	Description
`brief`	Enables brief debug mode.
`full`	Enables full debug mode.

Default SSH client debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Examples To start SSH client debugging, use the command:

```
awplus# debug ssh client
```

To start SSH client debugging with extended output, use the command:

```
awplus# debug ssh client full
```

To disable SSH client debugging, use the command:

```
awplus# no debug ssh client
```

Related Commands

debug ssh server

show ssh client

undebug ssh client

debug ssh server

Overview This command enables the SSH server debugging facility. When enabled, the SSH server sends diagnostic messages to the system log. To display the debugging messages on the terminal, use the **terminal monitor** command.

The **no** variant of this command disables the SSH server debugging facility. This stops the SSH server from generating diagnostic debugging messages.

Syntax

```
debug ssh server [brief|full]
no debug ssh server
```

Parameter	Description
`brief`	Enables brief debug mode.
`full`	Enables full debug mode.

Default SSH server debugging is disabled by default.

Mode Privileged Exec and Global Configuration

Examples To start SSH server debugging, use the command:

```
awplus# debug ssh server
```

To start SSH server debugging with extended output, use the command:

```
awplus# debug ssh server full
```

To disable SSH server debugging, use the command:

```
awplus# no debug ssh server
```

Related Commands

debug ssh client

show ssh server

undebug ssh server

service ssh

Overview This command enables the Secure Shell server on the device. Once enabled, connections coming from SSH clients are accepted.

SSH server needs a host key before it starts. If an SSHv2 host key does not exist, then this command fails. If SSHv1 is enabled but a host key for SSHv1 does not exist, then SSH service is unavailable for version 1.

The **no** variant of this command disables the Secure Shell server. When the Secure Shell server is disabled, connections from SSH, SCP, and SFTP clients are not accepted. This command does not affect existing SSH sessions. To terminate existing sessions, use the clear ssh command.

Syntax

```
service ssh [ip|ipv6]
no service ssh [ip|ipv6]
```

Default The Secure Shell server is disabled by default. Both IPv4 and IPv6 Secure Shell server are enabled when you issue **service ssh** without specifying the optional **ip** or **ipv6** parameters.

Mode Global Configuration

Examples To enable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh
```

To enable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ip
```

To enable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# service ssh ipv6
```

To disable both the IPv4 and the IPv6 Secure Shell server, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh
```

To disable the IPv4 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ip
```

To disable the IPv6 Secure Shell server only, use the commands:

```
awplus# configure terminal
awplus(config)# no service ssh ipv6
```

Related Commands

crypto key generate hostkey

show running-config ssh

show ssh server

ssh server allow-users

ssh server deny-users

show banner login

Overview This command displays the banner message configured on the device. The banner message is displayed to the remote user before user authentication starts.

Syntax

```
show banner login
```

Mode User Exec, Privileged Exec, Global Configuration, Interface Configuration, Line Configuration

Example To display the current login banner message, use the command:

```
awplus# show banner login
```

Related Commands banner login (SSH)

show crypto key hostkey

Overview This command displays the SSH host keys generated by RSA and DSA algorithm.

A host key pair (public and private keys) is needed to enable SSH server. The private key remains on the device secretly. The public key is copied to SSH clients to identify the server

Syntax

```
show crypto key hostkey [dsa|rsa|rsa1]
```

Parameter	Description
dsa	Displays the DSA algorithm public key.
rsa	Displays the RSA algorithm public key for SSH version 2 connections.
rsa1	Displays the RSA algorithm public key for SSH version 1 connections.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public keys generated on the device for SSH server, use the command:

```
awplus# show crypto key hostkey
```

To display the RSA public key of the SSH server, use the command:

```
awplus# show crypto key hostkey rsa
```

Output Figure 48-1: Example output from the **show crypto key hostkey** command

```
Type Bits   Fingerprint
-----------------------------------------------------------
rsa  2058   4e:7d:1d:00:75:79:c5:cb:c8:58:2e:f9:29:9c:1f:48
dsa  1024   fa:72:3d:78:35:14:cb:9a:1d:ca:1c:83:2c:7d:08:43
rsa1 1024   e2:1c:c8:8b:d8:6e:19:c8:f4:ec:00:a2:71:4e:85:8b
```

Table 1: Parameters in output of the **show crypto key hostkey** command

Parameter	Description
Type	Algorithm used to generate the key.
Bits	Length in bits of the key.
Fingerprint	Checksum value for the public key.

Related Commands

crypto key destroy hostkey

crypto key generate hostkey

show crypto key pubkey-chain knownhosts

Overview This command displays the list of public keys maintained in the known host database on the device.

Syntax

```
show crypto key pubkey-chain knownhosts [<1-65535>]
```

Parameter	Description
<1-65535>	Key identifier for a specific key. Displays the public key of the entry if specified.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Examples To display public keys of known SSH servers, use the command:

```
awplus# show crypto key pubkey-chain knownhosts
```

To display the key data of the first entry in the known host data, use the command:

```
awplus# show crypto key pubkey-chain knownhosts 1
```

Output Figure 48-2: Example output from the**show crypto key public-chain knownhosts** command

```
No    Hostname         Type Fingerprint
-------------------------------------------------------------------
1     172.16.23.1      rsa  c8:33:b1:fe:6f:d3:8c:81:4e:f7:2a:aa:a5:be:df:18
2     172.16.23.10     rsa  c4:79:86:65:ee:a0:1d:a5:6a:e8:fd:1d:d3:4e:37:bd
3     5ffe:1053:ac21:ff00:0101:bcdf:ffff:0001
                       rsa1 af:4e:b4:a2:26:24:6d:65:20:32:d9:6f:32:06:ba:57
```

Table 2: Parameters in the output of the **show crypto key public-chain knownhosts** command

Parameter	Description
`No`	Number ID of the key.
`Hostname`	Host name of the known SSH server.
`Type`	The algorithm used to generate the key.
`Fingerprint`	Checksum value for the public key.

Related Commands crypto key pubkey-chain knownhosts

show crypto key pubkey-chain userkey

Overview This command displays the public keys registered with the SSH server for SSH users. These keys allow remote users to access the device using public key authentication. By using public key authentication, users can access the SSH server without providing password.

Syntax

```
show crypto key pubkey-chain userkey <username> [<1-65535>]
```

Parameter	Description
<username>	User name of the remote SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
<1-65535>	Key identifier for a specific key.

Default Display all keys.

Mode User Exec, Privileged Exec and Global Configuration

Example To display the public keys for the user `manager` that are registered with the SSH server, use the command:

```
awplus# show crypto key pubkey-chain userkey manager
```

Output Figure 48-3: Example output from the **show crypto key public-chain userkey** command

```
No Type Bits Fingerprint
-------------------------------------------------------------------
1  dsa  1024 2b:cc:df:a8:f8:2e:8f:a4:a5:4f:32:ea:67:29:78:fd
2  rsa  2048 6a:ba:22:84:c1:26:42:57:2c:d7:85:c8:06:32:49:0e
```

Table 3: Parameters in the output of the **show crypto key userkey** command

Parameter	Description
`No`	Number ID of the key.
`Type`	The algorithm used to generate the key.
`Bits`	Length in bits of the key.
`Fingerprint`	Checksum value for the key.

Related Commands crypto key pubkey-chain userkey

show crypto key userkey

Overview This command displays the public keys created on this device for the specified SSH user.

Syntax

```
show crypto key userkey <username> [dsa|rsa|rsa1]
```

Parameter	Description
<username>	User name of the local SSH user whose keys you wish to display. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen and full stop symbols.
dsa	Displays the DSA public key.
rsa	Displays the RSA public key used for SSH version 2 connections.
rsa1	Displays the RSA key used for SSH version 1 connections.

Mode User Exec, Privileged Exec and Global Configuration

Examples To show the public key generated for the user, use the command:

```
awplus# show crypto key userkey manager
```

To store the RSA public key generated for the user manager to the file “user.pub”, use the command:

```
awplus# show crypto key userkey manager rsa > manager-rsa.pub
```

Output Figure 48-4: Example output from the **show crypto key userkey** command

```
Type Bits   Fingerprint
-----------------------------------------------------------
rsa  2048   e8:d6:1b:c0:f4:b6:e6:7d:02:2e:a9:d4:a1:ca:3b:11
rsa1 1024   12:25:60:95:64:08:8e:a1:8c:3c:45:1b:44:b9:33:9b
```

Table 4: Parameters in the output of the **show crypto key userkey** command

Parameter	Description
Type	The algorithm used to generate the key.
Bits	Length in bits of the key.
Fingerprint	Checksum value for the key.

Related Commands crypto key generate userkey

show running-config ssh

Overview This command displays the current running configuration of Secure Shell (SSH).

Syntax

```
show running-config ssh
```

Mode Privileged Exec and Global Configuration

Example To display the current configuration of SSH, use the command:

```
awplus# show running-config ssh
```

Output Figure 48-5: Example output from the **show running-config ssh** command

```
!
ssh server session-timeout 600
ssh server login-timeout 30
ssh server allow-users manager 192.168.1.*
ssh server allow-users john
ssh server deny-user john*.a-company.com
ssh server
```

Table 5: Parameters in the output of the **show running-config ssh** command

Parameter	Description
`ssh server`	SSH server is enabled.
`ssh server v2`	SSH server is enabled and only support SSHv2.
`ssh server<port>`	SSH server is enabled and listening on the specified TCP port.
`no ssh server scp`	SCP service is disabled.
`no ssh server sftp`	SFTP service is disabled.
`ssh server session-timeout`	Configure the server session timeout.
`ssh server login-timeout`	Configure the server login timeout.
`ssh server max-startups`	Configure the maximum number of concurrent sessions waiting authentication.
`no ssh server authentication password`	Password authentication is disabled.
`no ssh server authentication publickey`	Public key authentication is disabled.

Table 5: Parameters in the output of the **show running-config ssh** command

Parameter	Description
`ssh server allow-users`	Add the user (and hostname) to the allow list.
`ssh server deny-users`	Add the user (and hostname) to the deny list.

Related Commands

service ssh

show ssh server

show ssh

Overview This command displays the active SSH sessions on the device, both incoming and outgoing.

Syntax

```
show ssh
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current SSH sessions on the device, use the command:

```
awplus# show ssh
```

Output Figure 48-6: Example output from the **show ssh** command

```
Secure Shell Sessions:
ID  Type Mode   Peer Host    Username   State       Filename
-----------------------------------------------------------------
414 ssh  server 172.16.23.1  root       open
456 ssh  client 172.16.23.10 manager    user-auth
459 scp  client 172.16.23.12 root       download    550dev_.awd
463 ssh  client 5ffe:33fe:5632:ffbb:bc35:ddee:0101:ac51
                             manager    user-auth
```

Table 6: Parameters in the output of the **show ssh** command

Parameter	Description
ID	Unique identifier for each SSH session.
Type	Session type; either SSH, SCP, or SFTP.
Mode	Whether the device is acting as an SSH client (client) or SSH server (server) for the specified session.
Peer Host	The hostname or IP address of the remote server or client.
Username	Login user name of the server.

Table 6: Parameters in the output of the **show ssh** command (cont.)

Parameter	Description	
State	The current state of the SSH session. One of:	
	connecting	The device is looking for a remote server.
	connected	The device is connected to the remote server.
	accepted	The device has accepted a new session.
	host-auth	host-to-host authentication is in progress.
	user-auth	User authentication is in progress.
	authenticated	User authentication is complete.
	open	The session is in progress.
	download	The user is downloading a file from the device.
	upload	The user is uploading a file from the device.
	closing	The user is terminating the session.
	closed	The session is closed.
Filename	Local filename of the file that the user is downloading or uploading.	

Related Commands clear ssh

show ssh client

Overview This command displays the current configuration of the Secure Shell client.

Syntax

```
show ssh client
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current configuration for SSH clients on the login shell, use the command:

```
awplus# show ssh client
```

Output Figure 48-7: Example output from the **show ssh client** command

```
Secure Shell Client Configuration
-----------------------------------------------------------------
Port                            : 22
Version                         : 2,1
Connect Timeout                 : 30 seconds
Session Timeout                 : 0 (off)
Debug                           : NONE
```

Table 7: Parameters in the output of the **show ssh client** command

Parameter	Description
Port	SSH server TCP port where the SSH client connects to. The default is port 22.
Version	SSH server version; either “1”, “2” or “2,1”.
Connect Timeout	Time in seconds that the SSH client waits for an SSH session to establish. If the value is 0, the connection is terminated when it reaches the TCP timeout.
Debug	Whether debugging is active on the client.

Related Commands show ssh server

show ssh server

Overview This command displays the current configuration of the Secure Shell server.

Note that changes to the SSH configuration affects only new SSH sessions coming from remote hosts, and does not affect existing sessions.

Syntax

```
show ssh server
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the current configuration of the Secure Shell server, use the command:

```
awplus# show ssh server
```

Output Figure 48-8: Example output from the **show ssh server** command

```
Secure Shell Server Configuration
-----------------------------------------------------------------
SSH Server                          : Enabled
Port                                : 22
Version                             : 2
Services                            : scp, sftp
User Authentication                 : publickey, password
Resolve Hosts                       : Disabled
Session Timeout                     : 0 (Off)
Login Timeout                       : 60 seconds
Maximum Authentication Tries        : 6
Maximum Startups                    : 10
Debug                               : NONE
```

Table 8: Parameters in the output of the **show ssh server** command

Parameter	Description
SSH Server	Whether the Secure Shell server is enabled or disabled.
Port	TCP port where the Secure Shell server listens for connections. The default is port 22.
Version	SSH server version; either “1”, “2” or “2,1”.
Services	List of the available Secure Shell service; one or more of SHELL, SCP or SFTP.
Authentication	List of available authentication methods.
Login Timeout	Time (in seconds) that the SSH server will wait the SSH session to establish. If the value is 0, the client login will be terminated when TCP timeout reaches.

Table 8: Parameters in the output of the **show ssh server** command (cont.)

Parameter	Description
`Idle Timeout`	Time (in seconds) that the SSH server will wait to receive data from the SSH client. The server disconnects if this timer limit is reached. If set at 0, the idle timer remains off.
`Maximum Startups`	The maximum number of concurrent connections that are waiting authentication. The default is 10.
`Debug`	Whether debugging is active on the server.

Related Commands

show ssh

show ssh client

show ssh server allow-users

Overview This command displays the user entries in the allow list of the SSH server.

Syntax

```
show ssh server allow-users
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the user entries in the allow list of the SSH server, use the command:

```
awplus# show ssh server allow-users
```

Output Figure 48-9: Example output from the **show ssh server allow-users** command

```
Username          Remote Hostname (pattern)
----------------- ------------------------------
awplus            192.168.*
john
manager           *.alliedtelesis.com
```

Table 9: Parameters in the output of the **show ssh server allow-users** command

Parameter	Description
`Username`	User name that is allowed to access the SSH server.
`Remote Hostname (pattern)`	IP address or hostname pattern of the remote client. The user is allowed requests from a host that matches this pattern. If no hostname is specified, the user is allowed from all hosts.

Related Commands

ssh server allow-users

ssh server deny-users

show ssh server deny-users

Overview This command displays the user entries in the deny list of the SSH server. The user in the deny list is rejected to access the SSH server. If a user is not included in the access list of the SSH server, the user is also rejected.

Syntax

```
show ssh server deny-users
```

Mode User Exec, Privileged Exec and Global Configuration

Example To display the user entries in the deny list of the SSH server, use the command:

```
awplus# show ssh server deny-users
```

Output Figure 48-10: Example output from the **show ssh server deny-users** command

```
Username          Remote Hostname (pattern)
----------------- --------------------------------
john              *.b-company.com
manager           192.168.2.*
```

Table 10: Parameters in the output of the **show ssh server deny-user** command

Parameter	Description
Username	The user that this rule applies to.
Remote Hostname (pattern)	IP address or hostname pattern of the remote client. The user is denied requests from a host that matches this pattern. If no hostname is specified, the user is denied from all hosts.

Related Commands

ssh server allow-users

ssh server deny-users

ssh

Overview This command initiates a Secure Shell connection to a remote SSH server.

If the server requests a password for the user login, the user needs to type in the correct password on “Password:” prompt.

SSH client identifies the remote SSH server by its public key registered on the client device. If the server identification is changed, server verification fails. If the public key of the server has been changed, the public key of the server must be explicitly added to the known host database.

NOTE: *Note that a hostname specified with SSH cannot begin with a hyphen (-) character.*

Syntax

```
ssh [ip|ipv6][{[user <username>]|[port <1-65535>]|[version
{1|2]}}] <hostname> [<line>]
```

Parameter	Description	
`ip`	Specify IPv4 SSH.	
`ipv6`	Specify IPv6 SSH.	
`user`	Login user. If user is specified, the username is used for login to the remote SSH server when user authentication is required. Otherwise the current user name is used.	
	<username>	User name to login on the remote server.
`port`	SSH server port. If port is specified, the SSH client connects to the remote SSH server with the specified TCP port. Other- wise, the client port configured by “ssh client” command or the default TCP port (22) is used.	
	<1-65535>	TCP port.
`version`	SSH client version. If version is specified, the SSH client supports only the specified SSH version. By default, SSH client uses SSHv2 first. If the server does not support SSHv2, it will try SSHv1. The default version can be configured by “ssh client” command.	
	`1`	Use SSH version 1.
	`2`	Use SSH version 2.
<hostname>	IPv4/IPv6 address or hostname of a remote server. The address is in the format A.B.C.D for an IPv4 address, or in the format X:X::X:X for an IPv6 address. Note that a hostname specified with SSH cannot begin with a hyphen (-) character.	
<line>	A command to execute on the remote server. If a command is specified, the command is executed on the remote SSH server and the session is disconnected when the remote command finishes.	

Mode User Exec and Privileged Exec

Examples

To login to the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 as user “manager”, use the command:

```
awplus# ssh ip user manager 192.0.2.5
```

To login to the remote SSH server at 192.0.2.5 that is listening TCP port 2000, use the command:

```
awplus# ssh port 2000 192.0.2.5
```

To login to the remote SSH server with example_host using IPv6 session, use the command:

```
awplus# ssh ipv6 example_host
```

To run the **cmd** command on the remote SSH server at 192.0.2.5, use the command:

```
awplus# ssh ip 192.0.2.5 cmd
```

Related Commands

crypto key generate userkey

crypto key pubkey-chain knownhosts

debug ssh client

ssh client

ssh client

Overview This command modifies the default configuration parameters of the Secure Shell (SSH) client. The configuration is used for any SSH client on the device to connect to remote SSH servers. Any parameters specified on SSH client explicitly override the default configuration parameters.

The change affects the current user shell only. When the user exits the login session, the configuration does not persist. This command does not affect existing SSH sessions.

The **no** variant of this command resets configuration parameters of the Secure Shell (SSH) client changed by the ssh client command, and restores the defaults.

This command does not affect the existing SSH sessions.

Syntax

```
ssh client {port <1-65535>|version {1|2}|session-timeout
<0-3600>|connect-timeout <1-600>}
```

```
no ssh client {port|version|session-timeout|connect-timeout}
```

Parameter	Description	
`port`	The default TCP port of the remote SSH server. If an SSH client specifies an explicit port of the server, it overrides the default TCP port. Default: 22	
	<1-65535>	TCP port number.
`version`	The SSH version used by the client for SSH sessions. The SSH client supports both version 2 and version 1 Default: version 2 Note: SSH version 2 is the default SSH version. SSH client supports SSH version 1 if SSH version 2 is not configured using a ssh version command.	
	`1`	SSH clients on the device supports SSH version 1 only.
	`2`	SSH clients on the device supports SSH version 2 only
`session-timeout`	The global session timeout for SSH sessions. If the session timer lapses since the last time an SSH client received data from the remote server, the session is terminated. If the value is 0, then the client does not terminate the session. Instead, the connection is terminated when it reaches the TCP timeout. Default: 0 (session timer remains off)	
	<0-3600>	Timeout in seconds.

Parameter	Description
`connect-timeout`	The maximum time period that an SSH session can take to become established. The SSH client terminates the SSH session if this timeout expires and the session is still not established. Default: 30
	<1-600> Timeout in seconds.

Mode Privileged Exec

Examples To configure the default TCP port for SSH clients to 2200, and the session timer to 10 minutes, use the command:

```
awplus# ssh client port 2200 session-timeout 600
```

To configure the connect timeout of SSH client to 10 seconds, use the command:

```
awplus# ssh client connect-timeout 10
```

To restore the connect timeout to its default, use the command:

```
awplus# no ssh client connect-timeout
```

Related Commands show ssh client

ssh

ssh server

Overview This command modifies the configuration of the SSH server. Changing these parameters affects new SSH sessions connecting to the device.

The **no** variant of this command restores the configuration of a specified parameter to its default. The change affects the SSH server immediately if the server is running. Otherwise, the configuration is used when the server starts.

To enable the SSH server, use the service ssh command.

Syntax

```
ssh server {[v1v2|v2only]|<1-65535>}
ssh server {[session-timeout <0-3600>] [login-timeout <1-600>]
[max-startups <1-128>]}
no ssh server {[session-timeout] [login-timeout]
[max-startups]}
```

Parameter	Description
`v1v2`	Supports both SSHv2 and SSHv1client connections. Default: v1v2
`v2only`	Supports SSHv2 client connections only.
<1-65535>	The TCP port number that the server listens to for incoming SSH sessions. Default: 22
`session-timeout`	There is a maximum time period that the server waits before deciding that a session is inactive and should be terminated. The server considers the session inactive when it has not received any data from the client, and when the client does not respond to keep alive messages. Default: 0 (session timer remains off).
	<0-3600> Timeout in seconds.
`login-timeout`	The maximum time period the server waits before disconnecting an unauthenticated client. Default: 60
	<1-600> Timeout in seconds.
`max-startups`	The maximum number of concurrent unauthenticated connections the server accepts. When the number of SSH connections awaiting authentication reaches the limit, the server drops any additional connections until authentication succeeds or the login timer expires for a connection. Default: 10
	<1-128> Number of sessions.

Mode Global Configuration

Examples

To configure the session timer of SSH server to 10 minutes (600 seconds), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 600
```

To configure the login timeout of SSH server to 30 seconds, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server login-timeout 30
```

To limit the number of SSH client connections waiting authentication from SSH server to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-startups
```

To set max-startups parameters of SSH server to the default configuration, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server max-startups
```

To support the Secure Shell server with TCP port 2200, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server 2200
```

To force the Secure Shell server to support SSHv2 only, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v2only
```

To support both SSHv2 and SSHv1, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server v1v2
```

Related Commands

show ssh server

ssh client

ssh server allow-users

Overview This command adds a username pattern to the allow list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is accepted.

When there are no registered users in the server's database of allowed users, the SSH server does not accept SSH sessions even when enabled.

SSH server also maintains the deny list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

The **no** variant of this command deletes a username pattern from the allow list of the SSH server. To delete an entry from the allow list, the username and hostname pattern should match exactly with the existing entry.

Syntax

```
ssh server allow-users <username-pattern> [<hostname-pattern>]
no ssh server allow-users <username-pattern>
[<hostname-pattern>]
```

Parameter	Description
<username-pattern>	The username pattern that users can match to. An asterisk acts as a wildcard character that matches any string of characters.
<hostname-pattern>	The host name pattern that hosts can match to. If specified, the server allows the user to connect only from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.

Mode Global Configuration

Examples To allow the user `john` to create an SSH session from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john
```

To allow the user `john` to create an SSH session from a range of IP address (from 192.168.1.1 to 192.168.1.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john 192.168.1.*
```

To allow the user `john` to create a SSH session from `a-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server allow-users john *.a-company.com
```

To delete the existing user entry `john 192.168.1.*` in the allow list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server allow-users john 192.168.1.*
```

Related Commands

show running-config ssh

show ssh server allow-users

ssh server deny-users

ssh server authentication

Overview This command enables RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **ssh server authentication** command to enable password authentication for users. Apply the **publickey** keyword with the **ssh server authentication** command to enable RSA public-key authentication for users.

Use the **no** variant of this command to disable RSA public-key or password user authentication for SSH Server. Apply the **password** keyword with the **no ssh authentication** command to disable password authentication for users. Apply the required **publickey** keyword with the **no ssh authentication** command to disable RSA public-key authentication for users.

Syntax

```
ssh server authentication {password|publickey}
no ssh server authentication {password|publickey}
```

Parameter	Description
`password`	Specifies user password authentication for SSH server.
`publickey`	Specifies user publickey authentication for SSH server.

Default Both RSA public-key authentication and password authentication are enabled by default.

Mode Global Configuration

Usage For password authentication to authenticate a user, password authentication for a user must be registered in the local user database or on an external RADIUS server, before using the **ssh server authentication password** command.

For RSA public-key authentication to authenticate a user, a public key must be added for the user, before using the **ssh server authentication publickey** command.

Examples To enable `password` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication password
```

To enable `publickey` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server authentication publickey
```

To disable `password` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication password
```

To disable `publickey` authentication for users connecting through SSH, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server authentication publickey
```

Related Commands

crypto key pubkey-chain userkey

service ssh

show ssh server

ssh server deny-users

Overview This command adds a username pattern to the deny list of the SSH server. If the user of an incoming SSH session matches the pattern, the session is rejected.

SSH server also maintains the allow list. The server checks the user in the deny list first. If a user is listed in the deny list, then the user access is denied even if the user is listed in the allow list.

If a hostname pattern is specified, the user is denied from the hosts matching the pattern.

The **no** variant of this command deletes a username pattern from the deny list of the SSH server. To delete an entry from the deny list, the username and hostname pattern should match exactly with the existing entry.

Syntax

```
ssh server deny-users <username-pattern> [<hostname-pattern>]
no ssh server deny-users <username-pattern>
[<hostname-pattern>]
```

Parameter	Description
<username-pattern>	The username pattern that users can match to. The username must begin with a letter. Valid characters are all numbers, letters, and the underscore, hyphen, full stop and asterisk symbols. An asterisk acts as a wildcard character that matches any string of characters.
<hostname-pattern>	The host name pattern that hosts can match to. If specified, the server denies the user only when they connect from hosts matching the pattern. An asterisk acts as a wildcard character that matches any string of characters.

Mode Global Configuration

Examples To deny the user `john` to access SSH login from any host, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john
```

To deny the user john to access SSH login from a range of IP address (from 192.168.2.1 to 192.168.2.255), use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john 192.168.2.*
```

To deny the user `john` to access SSH login from `b-company.com` domain, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server deny-users john*.b-company.com
```

To delete the existing user entry `john 192.168.2.*` in the deny list, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server deny-users john 192.168.2.*
```

Related Commands

show running-config ssh

show ssh server deny-users

ssh server allow-users

ssh server max-auth-tries

Overview Use this command to specify the maximum number of SSH authentication attempts that the device will allow.

Use the **no** variant of this command to return the maximum number of attempts to its default value of 6.

Syntax

```
ssh server max-auth-tries <1-32>
no ssh server max-auth-tries
```

Parameter	Description
<1-32>	Maximum number of SSH authentication attempts the device will allow.

Default 6 attempts

Mode Global Configuration

Usage By default, users must wait one second after a failed login attempt before trying again. You can increase this gap by using the command aaa login fail-delay.

Example To set the maximum number of SSH authentication attempts to 3, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server max-auth-tries 3
```

Related Commands show ssh server

ssh server resolve-host

Overview This command enables resolving an IP address from a host name using a DNS server for client host authentication.

The **no** variant of this command disables this feature.

Syntax

```
ssh server resolve-hosts
no ssh server resolve-hosts
```

Default This feature is disabled by default.

Mode Global Configuration

Usage Your device has a DNS Client that is enabled automatically when you add a DNS server to your device. Use the ip name-server command to add a DNS server to the list of servers that the device queries.

For information about configuring DNS, see the Internet Protocol Feature Overview and Configuration Guide.

Example To resolve a host name using a DNS server, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server resolve-hosts
```

Related Commands

ip name-server

show ssh server

ssh server allow-users

ssh server deny-users

ssh server scp

Overview This command enables the Secure Copy (SCP) service on the SSH server. Once enabled, the server accepts SCP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SCP connections. The SCP service is enabled by default as soon as the SSH server is enabled.

The **no** variant of this command disables the SCP service on the SSH server. Once disabled, SCP requests from remote clients are rejected.

Syntax

```
ssh server scp
no ssh server scp
```

Mode Global Configuration

Examples To enable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server scp
```

To disable the SCP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server scp
```

Related Commands show running-config ssh

show ssh server

ssh server sftp

Overview This command enables the Secure FTP (SFTP) service on the SSH server. Once enabled, the server accepts SFTP requests from remote clients.

You must enable the SSH server as well as this service before the device accepts SFTP connections. The SFTP service is enabled by default as soon as the SSH server is enabled. If the SSH server is disabled, SFTP service is unavailable.

The **no** variant of this command disables SFTP service on the SSH server. Once disabled, SFTP requests from remote clients are rejected.

Syntax

```
ssh server sftp
no ssh server sftp
```

Mode Global Configuration

Examples To enable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# ssh server sftp
```

To disable the SFTP service, use the commands:

```
awplus# configure terminal
awplus(config)# no ssh server sftp
```

Related Commands show running-config ssh

show ssh server

undebug ssh client

Overview This command applies the functionality of the **no** debug ssh client command.

undebug ssh server

Overview This command applies the functionality of the **no** debug ssh server command.

49 Trigger Commands

Introduction

Overview

This chapter provides an alphabetical reference for commands used to configure Triggers. For more information, see the Triggers Feature Overview and Configuration Guide.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Command List

active (trigger)

Overview This command enables a trigger. This allows the trigger to activate when its trigger conditions are met.

The **no** variant of this command disables a trigger. While in this state the trigger cannot activate when its trigger conditions are met.

Syntax

```
active
no active
```

Mode Trigger Configuration

Usage Configure a trigger first before you use this command to activate it.

For information about configuring a trigger, see the Triggers Feature Overview and Configuration Guide.

Examples To enable trigger 172, so that it can activate when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 172
awplus(config-trigger)# active
```

To disable trigger 182, preventing it from activating when its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 182
awplus(config-trigger)# no active
```

Related Commands show trigger

trigger

day

Overview This command specifies the days or date that the can trigger activate on. You can specify either:

- A specific date
- A specific day of the week
- A list of days of the week
- every day

By default, the trigger can activate on any day.

Syntax

```
day every-day
day <1-31> <month> <2000-2035>
day <weekday>
```

Parameter	Description
`every-day`	Sets the trigger so that it can activate on any day.
<1-31>	Day of the month the trigger is permitted to activate on.
<month>	Sets the month that the trigger is permitted to activate on. Valid keywords are: **january, february, march, april, may, june, july, august, september, october, november**, and **december**.
<2000-2035>	Sets the year that the trigger is permitted to activate in.
<weekday>	Sets the days of the week that the trigger can activate on. You can specify one or more week days in a space separated list. Valid keywords are: **monday, tuesday, wednesday, thursday, friday, saturday**, and **sunday**.

Mode Trigger Configuration

Usage For example trigger configurations that use the **day** command, see "Restrict Internet Access" and "Turn off Power to Port LEDs" in the Triggers Feature Overview and Configuration Guide.

Examples To permit trigger 55 to activate on the `1 Jun 2010`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 55
awplus(config-trigger)# day 1 Jun 2010
```

To permit trigger 12 to activate on a Mondays, Wednesdays and Fridays, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# day monday wednesday friday
```

Related Commands

show trigger

trigger

debug trigger

Overview This command enables trigger debugging. This generates detailed messages about how your device is processing the trigger commands and activating the triggers.

The **no** variant of this command disables trigger debugging.

Syntax

```
debug trigger
no debug trigger
```

Mode Privilege Exec

Examples To start trigger debugging, use the command:

```
awplus# debug trigger
```

To stop trigger debugging, use the command:

```
awplus# no trigger
```

Related Commands

show debugging trigger

show trigger

test

trigger

undebug trigger

description (trigger)

Overview This command adds an optional description to help you identify the trigger. This description is displayed in show command outputs and log messages.

The **no** variant of this command removes a trigger's description. The show command outputs and log messages stop displaying a description for this trigger.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	A word or phrase that uniquely identifies this trigger or its purpose. Valid characters are any printable character and spaces, up to a maximum of 40 characters.

Mode Trigger Configuration

Examples To give trigger 240 the description `daily status report`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 240
awplus(config-trigger)# description daily status report
```

To remove the description from trigger `36`, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 36
awplus(config-trigger)# no description
```

Related Commands

show trigger

test

trigger

repeat

Overview This command specifies the number of times that a trigger is permitted to activate. This allows you to specify whether you want the trigger to activate:

- only the first time that the trigger conditions are met
- a limited number of times that the trigger conditions are met
- an unlimited number of times

Once the trigger has reached the limit set with this command, the trigger remains in your configuration but cannot be activated. Use the **repeat** command again to reset the trigger so that it is activated when its trigger conditions are met.

By default, triggers can activate an unlimited number of times. To reset a trigger to this default, specify either **yes** or **forever**.

Syntax

```
repeat {forever|no|once|yes|<1-4294967294>}
```

Parameter	Description
`yes|forever`	The trigger repeats indefinitely, or until disabled.
`no|once`	The trigger activates only once.
<1-4292967294>	The trigger repeats the specified number of times.

Mode Trigger Configuration

Examples To allow trigger `21` to activate only once, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 21
awplus(config-trigger)# repeat no
```

To allow trigger `22` to activate an unlimited number of times whenever its trigger conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 22
awplus(config-trigger)# repeat forever
```

To allow trigger `23` to activate only the first `10` times the conditions are met, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 23
awplus(config-trigger)# repeat 10
```

Related Commands show trigger

trigger

script

Overview This command specifies one or more scripts that are to be run when the trigger activates. You can add up to five scripts to a single trigger.

The sequence in which the trigger runs the scripts is specified by the number you set before the name of the script file. One script is executed completely before the next script begins.

Scripts may be either ASH shell scripts, indicated by a **.sh** filename extension suffix, or AlliedWare Plus™ scripts, indicated by a **.scp** filename extension suffix. AlliedWare Plus™ scripts only need to be readable.

The **no** variant of this command removes one or more scripts from the trigger's script list. The scripts are identified by either their name, or by specifying their position in the script list. The **all** parameter removes all scripts from the trigger.

Syntax

```
script <1-5> {<filename>}
no script {<1-5>|<filename>|all}
```

Parameter	Description
<1-5>	The position of the script in execution sequence. The trigger runs the lowest numbered script first.
<filename>	The path to the script file.

Mode Trigger Configuration

Examples To configure trigger 71 to run the script flash:/cpu_trig.sh in position 3 when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# script 3 flash:/cpu_trig.sh
```

To configure trigger 99 to run the scripts **flash:reconfig.scp**, **flash:cpu_trig.sh** and **flash:email.scp** in positions 2, 3 and 5 when the trigger activates, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 99
awplus(config-trigger)# script 2 flash:/reconfig.scp 3
flash:/cpu_trig.sh 5 flash:/email.scp
```

To remove the scripts 1, 3 and 4 from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script 1 3 4
```

To remove the script flash:/cpu_trig.sh from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script flash:/cpu_trig.sh
```

To remove all the scripts from trigger 71's script list, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 71
awplus(config-trigger)# no script all
```

Related Commands

show trigger

trigger

show debugging trigger

Overview This command displays the current status for trigger utility debugging. Use this command to show when trigger debugging has been turned on or off from the debug trigger command.

Syntax

```
show debugging trigger
```

Mode User Exec and Privileged Exec

Example To display the current configuration of trigger debugging, use the command:

```
awplus# show debugging trigger
```

Output Figure 49-1: Example output from the **show debugging trigger** command

```
awplus#debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is on

awplus#no debug trigger
awplus#show debugging trigger
Trigger debugging status:
  Trigger debugging is off
```

Related Commands debug trigger

show running-config trigger

Overview This command displays the current running configuration of the trigger utility.

Syntax

```
show running-config trigger
```

Mode Privileged Exec

Example To display the current configuration of the trigger utility, use the command:

```
awplus# show running-config trigger
```

Output Figure 49-2: Example output from the **show running-config trigger** command

```
 trigger 1
  type card in

type usb in
 trigger 2

type usb out
 !
```

Related Commands show trigger

show trigger

Overview This command displays configuration and diagnostic information about the triggers configured on the device. Specify the **show trigger** command without any options to display a summary of the configuration of all triggers.

Syntax `show trigger [<1-250>|counter|full]`

Parameter	Description
<1-250>	Displays detailed information about a specific trigger, identified by its trigger ID.
`counter`	Displays statistical information about all triggers.
`full`	Displays detailed information about all triggers.

Mode Privileged Exec

Example To get summary information about all triggers, use the following command:

```
awplus# show trigger
```

Table 1: Example output from the **show trigger** command

```
awplus#show trigger
TR# Type & Details       Name                 Ac Te Tr Repeat      #Scr Days/Date
-------------------------------------------------------------------------------
001 USB
(in)                                  Y  N  Y  Continuous  0    smtwtfs
002 USB
(out)                                 Y  N  Y  Continuous  0    smtwtfs
003 CPU (80% any)        Busy CPU             Y  N  Y  5           1    smtwtfs
005 Periodic (30 min)    Regular status check Y  N  N  Continuous  1    -mtwtf-
007 Memory (85% up)      High mem usage       Y  N  Y  8           1    smtwtfs
011 Time (00:01)         Weekend access       Y  N  Y  Continuous  1    ------s
013 Reboot                                    Y  N  Y  Continuous  2    smtwtfs
017 Interface (vlan1 ... Change config for... Y  N  Y  Once        1    2-apr-2008
019 Ping-poll (5 up)     Connection to svr1   Y  N  Y  Continuous  1    smtwtfs
-------------------------------------------------------------------------------
```

Table 2: Parameters in the output of the **show trigger** command

Parameter	Description
`TR#`	Trigger identifier (ID).
`Type & Details`	The trigger type, followed by the trigger details in brackets.

Table 2: Parameters in the output of the **show trigger** command (cont.)

Parameter	Description
Name	Descriptive name of the trigger configured with the description (trigger) command.
Ac	Whether the trigger is active (Y), or inactive (N).
Te	Whether the trigger is in test mode (Y) or not (N).
Tr	Whether or not the trigger is enabled to send SNMP traps. See the trap command.
Repeat	Whether the trigger repeats continuously, and if not, the configured repeat count for the trigger. To see the number of times a trigger has activated, use the show trigger <1-250> command.
#Scr	Number of scripts associated with the trigger.
Days/Date	Days or date when the trigger may be activated. For the days options, the days are shown as a seven character string representing Sunday to Saturday. A hyphen indicates days when the trigger cannot be activated.

To display detailed information about trigger 3, use the command:

```
awplus# show trigger 3
```

Figure 49-3: Example output from the **show trigger** command for a specific trigger

```
awplus#show trigger 3
Trigger Configuration Details
-------------------------------------------------------------
Trigger ..................... 1
Description ................. display cpu usage when pass 80%
Type and details ............ CPU (80% up)
Days ........................ 26-nov-2007
After ....................... 00:00:00
Before ...................... 23:59:59
Active ...................... Yes
Test ........................ No
Trap ........................ Yes
Repeat ...................... 123 (0)
Modified .................... Tue Dec 20 02:26:03 1977
Number of activations ....... 0
Last activation ............. not activated
Number of scripts ........... 1
  1. shocpu.scp
  2. <not configured>
  3. <not configured>
  4. <not configured>
  5. <not configured>
-------------------------------------------------------------
```

To display detailed information about all triggers, use the command:

```
awplus# show trigger full
```

Table 3: Example output from the **show trigger full** command

```
awplus#show trigger full
Trigger Configuration Details
-------------------------------------------------------------
 Trigger ..................... 1
 Description ................. <no description>
 Type and
details ............ USB (in)
 Days ........................ smtwtfs
 After ....................... 00:00:00
 Before ...................... 23:59:59
 Active ...................... Yes
 Test ........................ No
 Trap ........................ Yes
 Repeat ...................... Continuous
 Modified .................... Fri Sep  3 14:45:56 2010
 Number of activations ....... 0
 Last activation ............. not activated
 Number of scripts ........... 0
   1. <not configured>
   2. <not configured>
   3. <not configured>
   4. <not configured>
   5. <not configured>

 Trigger ..................... 2
 Description ................. <no description>
 Type and
details ............ USB (out)
 Days ........................ smtwtfs
 After ....................... 00:00:00
 Before ...................... 23:59:59
 Active ...................... Yes
 Test ........................ No
 Trap ........................ Yes
 Repeat ...................... Continuous
 Modified .................... Fri Sep  3 14:45:56 2010
 Number of activations ....... 0
 Last activation ............. not activated
 Number of scripts ........... 0
   1. <not configured>
   2. <not configured>
   3. <not configured>
   4. <not configured>
   5. <not configured>
```

Table 4: Parameters in the output of the s**how trigger full** and **show trigger** commands for a specific trigger

Parameter	Description
`Trigger`	The ID of the trigger.
`Description`	Descriptive name of the trigger.
`Type and details`	The trigger type and its activation conditions.
`Days`	The days on which the trigger is permitted to activate.
`Date`	The date on which the trigger is permitted to activate. Only displayed if configured, in which case it replaces "Days".
`Active`	Whether or not the trigger is permitted to activate.
`Test`	Whether or not the trigger is operating in diagnostic mode.
`Trap`	Whether or not the trigger is enabled to send SNMP traps.
`Repeat`	Whether the trigger repeats an unlimited number of times (Continuous) or for a set number of times. When the trigger can repeat only a set number of times, then the number of times the trigger has been activated is displayed in brackets.
`Modified`	The date and time of the last time that the trigger was modified.
`Number of activations`	Number of times the trigger has been activated since the last restart of the device.
`Last activation`	The date and time of the last time that the trigger was activated.
`Number of scripts`	How many scripts are associated with the trigger, followed by the names of the script files in the order in which they run.

To display counter information about all triggers use the command:

```
awplus# show trigger counter
```

Figure 49-4: Example output from the **show trigger counter** command

```
awplus#show trigger counter
Trigger Module Counters
-----------------------------------------------------
Trigger activations ........................... 0
Time triggers activated today ................. 0
Periodic triggers activated today ............. 0
Interface triggers activated today ............ 0
Resource triggers activated today ............. 0
Reboot triggers activated today ............... 0
Ping-poll triggers activated today ............ 0
Stack
master fail triggers activated today .... 0
Stack
member triggers activated today ......... 0
-----------------------------------------------------
```

Table 5: Parameters in the output of the **show trigger counter** command

Parameter	Description
`Trigger activations`	Number of times a trigger has been activated.
`Time triggers activated today`	Number of times a time trigger has been activated today.
`Periodic triggers activated today`	Number of times a periodic trigger has been activated today.
`Interface triggers activated today`	Number of times an interface trigger has been activated today.
`Resource triggers activated today`	Number of times a CPU or memory resource trigger has been activated today.
`Ping-poll triggers activated today`	Number of times a ping-poll trigger has been activated today.

Related Commands trigger

test

Overview This command puts the trigger into a diagnostic mode. In this mode the trigger may activate but when it does it will not run any of the trigger's scripts. A log message will be generated to indicate when the trigger has been activated.

The **no** variant of this command takes the trigger out of diagnostic mode, restoring normal operation. When the trigger activates the scripts associated with the trigger will be run, as normal.

Syntax

```
test
no test
```

Mode Trigger Configuration

Usage Configure a trigger first before you use this command to diagnose it. For information about configuring a trigger, see the Triggers Feature Overview and Configuration Guide.

Examples To put trigger 5 into diagnostic mode, where no scripts will be run when the trigger activates, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# test
```

To take trigger 205 out of diagnostic mode, restoring normal operation, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no test
```

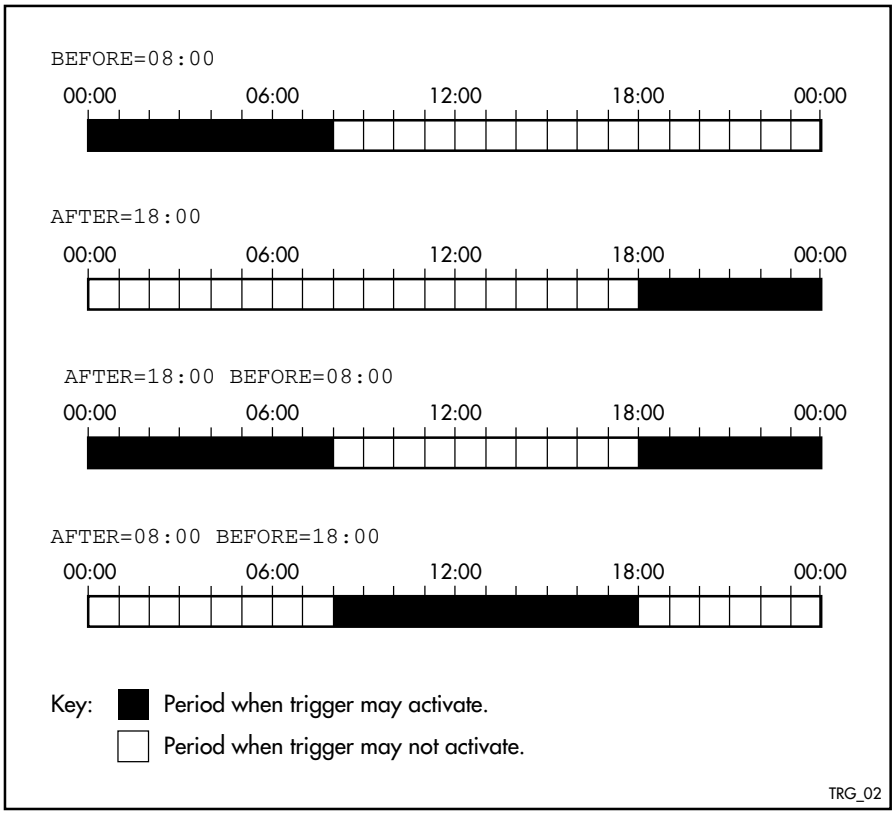
Related Commands show trigger

trigger

time (trigger)

Overview This command specifies the time of day when the trigger is permitted to activate. The after parameter specifies the start of a time period that extends to midnight during which trigger may activate. By default the value of this parameter is 00:00:00 (am); that is, the trigger may activate at any time. The **before** parameter specifies the end of a time period beginning at midnight during which the trigger may activate. By default the value of this parameter is 23:59:59; that is, the trigger may activate at any time. If the value specified for **before** is later than the value specified for **after**, a time period from **"** after **"** to **"** before **"** is defined, during which the trigger may activate. This command is not applicable to time triggers (**type time**).

The following figure illustrates how the **before** and **after** parameters operate.



Syntax `time {[after <hh:mm:ss>] [before <hh:mm:ss>]}`

Parameter	Description
`after`*<hh:mm:ss>*	The earliest time of day when the trigger may be activated.
`before`*<hh:mm:ss>*	The latest time of day when the trigger may be activated.

Mode Trigger Configuration

Usage For example trigger configurations that use the **time (trigger)** command, see "Restrict Internet Access" and "Turn off Power to Port LEDs" in the Triggers Feature Overview and Configuration Guide.

Examples To allow trigger `63` to activate between midnight and 10:30am, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 63
awplus(config-trigger)# time before 10:30:00
```

To allow trigger `64` to activate between 3:45pm and midnight, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 64
awplus(config-trigger)# time after 15:45:00
```

To allow trigger `65` to activate between 10:30am and 8:15pm, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 65
awplus(config-trigger)# time after 10:30:00 before 20:15:00
```

Related Commands show trigger

trigger

trap

Overview This command enables the specified trigger to send SNMP traps.

Use the **no** variant of this command to disable the sending of SNMP traps from the specified trigger.

Syntax

```
trap
no trap
```

Default SNMP traps are enabled by default for all defined triggers.

Mode Trigger Configuration

Usage You must configure SNMP before using traps with triggers. For more information, see:

- Support for Allied Telesis Enterprise_MIBs_in_AlliedWare Plus, for information about which MIB objects are supported.
- the SNMP Feature Overview and Configuration_Guide.
- the SNMP Commands chapter.

Since SNMP traps are enabled by default for all defined triggers, a common usage will be for the **no** variant of this command to disable SNMP traps from a specified trap if the trap is only periodic. Refer in particular to AT-TRIGGER-MIB in the Support for Allied Telesis Enterprise_MIBs_in AlliedWare Plus for further information about the relevant SNMP MIB.

Examples To enable SNMP traps to be sent from trigger 5, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# trap
```

To disable SNMP traps being sent from trigger 205, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 205
awplus(config-trigger)# no trap
```

Related Commands trigger

show trigger

trigger

Overview This command is used to access the Trigger Configuration mode for the specified trigger. Once Trigger Configuration mode has been entered the trigger type information can be configured and the trigger scripts and other operational parameters can be specified. At a minimum the trigger type information must be specified before the trigger can become active.

The **no** variant of this command removes a specified trigger and all configuration associated with it.

Syntax

```
trigger <1-250>
no trigger <1-250>
```

Parameter	Description
<1-250>	A trigger ID.

Mode Global Configuration

Examples To enter trigger configuration mode for trigger `12` use the command:

```
awplus# trigger 12
```

To completely remove all configuration associated with trigger `12`, use the command:

```
awplus# no trigger 12
```

Related Commands show trigger

trigger activate

trigger activate

Overview This command is used to manually activate a specified trigger from the Privileged Exec mode, which has been configured with the **trigger** command from the Global Configuration mode.

Syntax

```
trigger activate <1-250>
```

Parameter	Description
<1-250>	A trigger ID.

Mode Privileged Exec

Usage This command manually activates a trigger without the normal trigger conditions being met.

The trigger is activated even if it is configured as inactive. The scripts associated with the trigger will be executed even if the trigger is in the diagnostic test mode.

Triggers activated manually do not have their repeat counts decremented or their 'last triggered' time updated, and do not result in updates to the '[type] triggers today' counters.

Example To manually activate trigger `12` use the command:

```
awplus# trigger activate 12
```

Related Commands show trigger

trigger

type atmf node

Overview This command configures a trigger to be activated at an AMF node join event or leave event.

Syntax

```
type atmf node {join|leave}
```

Parameter	Description
join	AMF node join event.
leave	AMF node leave event.

Mode Trigger Configuration

CAUTION: Only configure this trigger on one device because it is a network wide event.

Example 1 To configure trigger 5 to activate at an AMF node leave event, use the following commands. In this example the command is entered on node-1:

```
node1(config)# trigger 5
node1(config-trigger) type atmf node leave
```

Example 2 The following commands will configure trigger 5 to activate if an AMF node join event occurs on any node within the working set:

```
node1# atmf working-set group all
```

This command returns the following display:

```
====================
node1, node2, node3:
====================

Working set join
```

Note that the running the above command changes the prompt from the name of the local node, to the name of the AMF-Network followed, in square brackets, by the number of member nodes in the working set.

```
AMF-Net[3]# conf t
AMF-Net[3](config)# trigger 5
AMF-Net[3](config-trigger)# type atmf node leave
AMF-Net[3](config-trigger)# description "E-mail on AMF Exit"
AMF-Net[3](config-trigger)# active
```

Enter the name of the script to run at the trigger event.

```
AMF-Net[3](config-trigger)# script 1 email_me.scp
AMF-Net[3](config-trigger)# end
```

Display the trigger configurations

```
AMF-Net[3]# show trigger
```

This command returns the following display:

```
=======
node1:
=======

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
001 Periodic (2 min)   Periodic Status Chk  Y  N  Y Continuous  1   smtwtfs
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------

==============
Node2, Node3,
==============

TR# Type & Details     Description          Ac Te Tr Repeat     #Scr Days/Date
-------------------------------------------------------------------------------
005 ATMF node (leave)  E-mail on ATMF Exit  Y  N  Y Continuous  1   smtwtfs
-------------------------------------------------------------------------------
```

Display the triggers configured on each of the nodes in the AMF Network.

```
AMF-Net[3]# show running-config trigger
```

This command returns the following display:

```
========
Node1:
========

trigger 1
 type periodic 2
 script 1 atmf.scp
trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!

============
Node2, Node3:
============

trigger 5
 type atmf node leave
description "E-mail on ATMF Exit"
 script 1 email_me.scp
!
```

Related Commands show trigger

type cpu

Overview This command configures a trigger to activate based on CPU usage level. Selecting the **up** option causes the trigger to activate when the CPU usage exceeds the specified usage level. Selecting the **down** option causes the trigger to activate when CPU usage drops below the specified usage level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

Syntax

```
type cpu <1-100> [up|down|any]
```

Parameter	Description
<1-100>	The percentage of CPU usage at which to trigger.
`up`	Activate when CPU usage exceeds the specified level.
`down`	Activate when CPU usage drops below the specified level
`any`	Activate when CPU usage passes the specified level in either direction

Mode Trigger Configuration

Usage For an example trigger configuration that uses the **type cpu** command, see "Capture Unusual CPU and RAM Activity" in the Triggers Feature Overview and Configuration Guide.

Examples To configure trigger `28` to be a CPU trigger that activates when CPU usage exceeds 80% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 28
awplus(config-trigger)# type cpu 80 up
```

To configure trigger `5` to be a CPU trigger that activates when CPU usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 5
awplus(config-trigger)# type cpu 65 any
```

Related Commands show trigger

trigger

type interface

Overview This command configures a trigger to activate based on the link status of an interface. The trigger can be activated when the interface becomes operational by using the **up** option, or when the interface closes by using the **down** option. The trigger can also be configured to activate when either one of these events occurs by using the **any** option.

Syntax

```
type interface <interface> [up|down|any]
```

Parameter	Description
<interface>	Interface name. This can be the name of a device port, an eth-management port, or a VLAN.
up	Activate when interface becomes operational.
down	Activate when the interface closes.
any	Activate when any interface link status event occurs.

Mode Trigger Configuration

Example To configure trigger 19 to be an interface trigger that activates when port1.0.2 becomes operational, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 19
awplus(config-trigger)# type interface port1.0.2 up
```

Related Commands

show trigger

trigger

type memory

Overview This command configures a trigger to activate based on RAM usage level. Selecting the **up** option causes the trigger to activate when memory usage exceeds the specified level. Selecting the **down** option causes the trigger to activate when memory usage drops below the specified level. Selecting **any** causes the trigger to activate in both situations. The default is **any**.

Syntax

```
type memory <1-100> [up|down|any]
```

Parameter	Description
<1-100>	The percentage of memory usage at which to trigger.
`up`	Activate when memory usage exceeds the specified level.
`down`	Activate when memory usage drops below the specified level.
`any`	Activate when memory usage passes the specified level in either direction.

Mode Trigger Configuration

Examples To configure trigger `12` to be a memory trigger that activates when memory usage exceeds 50% use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 12
awplus(config-trigger)# type memory 50 up
```

To configure trigger `40` to be a memory trigger that activates when memory usage either rises above or drops below 65%, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65
```

or

```
awplus# configure terminal
awplus(config)# trigger 40
awplus(config-trigger)# type memory 65 any
```

Related Commands show trigger

trigger

type periodic

Overview This command configures a trigger to be activated at regular intervals. The time period between activations is specified in minutes.

Syntax

```
type periodic <1-1440>
```

Parameter	Description
<1-1440>	The number of minutes between activations.

Mode Trigger Configuration

Usage A combined limit of 10 triggers of the type periodic and time can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

For an example trigger configuration that uses the **type periodic** command, see "See Daily Statistics" in the Triggers Feature Overview and Configuration Guide.

Example To configure trigger `44` to activate periodically at `10` minute intervals use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 44
awplus(config-trigger)# type periodic 10
```

Related Commands

show trigger

trigger

type ping-poll

Overview This command configures a trigger that activates when Ping Polling identifies that a target device's status has changed. This allows you to run a configuration script when a device becomes reachable or unreachable.

Syntax

```
type ping-poll <1-100> {up|down}
```

Parameter	Description
<1-100>	The ping poll ID.
`up`	The trigger activates when ping polling detects that the target is reachable.
`down`	The trigger activates when ping polling detects that the target is unreachable.

Mode Trigger Configuration

Example To configure trigger `106` to activate when ping poll `12` detects that its target device is now unreachable, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 106
awplus(config-trigger)# type ping-poll 12 down
```

Related Commands show trigger

trigger

type reboot

Overview This command configures a trigger that activates when your device is rebooted.

Syntax

```
type reboot
```

Mode Trigger Configuration

Example To configure trigger `32` to activate when your device reboots, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 32
awplus(config-trigger)# type reboot
```

Related Commands show trigger

trigger

type stack disabled-master

Overview This command (configured to the stack) configures a trigger to activate on a stack member if it becomes the disabled master.

A disabled master has the same configuration as the active master, but has all its links shutdown.

Although this command could activate any trigger script, the intention here is that the script will reactivate the links from their previously shutdown state, to enable the user to manage the device. An appropriate trigger script must already exist that will apply the shutdown command on the deactivated links.

CAUTION: *It is important that any ports that are configured as trunked ports across master and stack members are disabled at their stack member termination when operating in the fallback configuration. Otherwise, the trunked ports will not function correctly on the device that is connected downstream.*

If the stack virtual-mac command command is enabled, the stack uses a virtual MAC address. The stack will always use this MAC address and the new elected master will still retain the originally configured virtual MAC address. If the **stack virtual-mac** command is disabled, the stack will use the MAC address of the current master. If the stack master fails, the stack MAC address changes to reflect the new master's MAC address. For more information about virtual MAC addresses, see the VCStack Feature Overview and Configuration Guide.

Syntax

```
type stack disabled-master
```

Mode Trigger Configuration

Examples To configure trigger `82` to activate on a device if it becomes the disabled master, use the commands. These commands enter the Trigger Configuration mode for trigger 82, specify the trigger type, and then specify the script to run.

```
awplus# configure terminal
awplus(config)# trigger 82
awplus(config-trigger)# type stack disabled master
awplus(config-trigger)# script 1 flash:/disabled.scp
awplus(config-trigger)# exit
```

Related Commands

stack disabled-master-monitoring

trigger

type stack disabled-master

type stack member

type stack link

type stack link

Overview This command (configured to the stack) initiates the action of a pre-configured trigger to occur when a stacking link is either activated or deactivated.

Syntax

```
type stack link {up|down}
```

Parameter	Description
up	Stack link up event
down	Stack link down event

Mode Trigger Configuration

Example To configure trigger 86 to activate when the stack link down event occurs, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack link down
```

Related Commands

show trigger

trigger

type stack master-fail

type stack master-fail

Overview This command (configured to the stack) initiates the action of a pre-configured trigger to occur when the stack enters the fail-over state.

Syntax
```
type stack master-fail
```

Mode Trigger Configuration

Example To configure trigger `86` to activate when stack master fail-over event occurs, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack master-fail
```

Related Commands
stack disabled-master-monitoring

trigger

type stack disabled-master

type stack member

type stack link

type stack member

Overview This command (configured to the stack) initiates the action of a pre-configured trigger to occur when a device either joins or leaves the stack.

Syntax

```
type stack member {join|leave}
```

Parameter	Description
`join`	Neighbor join event
`leave`	Neighbor leave event

Mode Trigger Configuration

Example To configure a pre-configured trigger number `86` to activate when a new device joins the stack.

Note that the number `86` has no particular significance: you can assign any (previously created) numbered trigger.

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type stack member join
```

Related Commands

trigger

type stack master-fail

type stack link

type time

Overview This command configures a trigger that activates at a specified time of day.

Syntax

```
type time <hh:mm>
```

Parameter	Description
<hh:mm>	The time to activate the trigger.

Mode Trigger Configuration

Usage A combined limit of 10 triggers of the type time and type periodic can be configured. If you attempt to add more than 10 triggers the following error message is displayed:

```
% Cannot configure more than 10 triggers with the type time or
periodic
```

Example To configure trigger `86` to activate at `15:53`, use the following commands:

```
awplus# configure terminal
awplus(config)# trigger 86
awplus(config-trigger)# type time 15:53
```

Related Commands

show trigger

trigger

type usb

Overview Use this command to configure a trigger that activates on either the removal or the insertion of a USB storage device.

Syntax

```
type usb {in|out}
```

Parameter	Description
`in`	Trigger activates on insertion of a USB storage device.
`out`	Trigger activates on removal of a USB storage device.

Mode Trigger Configuration

Usage USB triggers cannot execute script files from a USB storage device.

For example trigger configurations that use the **type usb** command, see "Capture Show Output and Save to a USB Storage Device" in the Triggers Feature Overview and Configuration Guide.

Examples To configure `trigger 1` to activate on the insertion of a USB storage device, use the commands:

```
awplus# configure terminal
awplus(config)# trigger 1
awplus(config-trigger)# type usb in
```

Related Commands

trigger

show running-config trigger

show trigger

undebug trigger

Overview This command applies the functionality of the **no** debug trigger command.

50 Ping-Polling Commands

Introduction

This chapter provides an alphabetical reference for commands used to configure Ping Polling. For more information, see the Ping Polling Feature Overview and Configuration Guide.

For information on filtering and saving command output, see "Controlling "show" Command Output" in the "Getting Started with AlliedWare Plus" Feature Overview and Configuration Guide.

Table 50-1: The following table lists the default values when configuring a ping poll

Default	Value
Critical-interval	1 second
Description	No description
Fail-count	5
Length	32 bytes
Normal-interval	30 seconds
Sample-size	5
Source-ip	The IP address of the interface from which the ping packets are transmitted
Time-out	1 second
Up-count	30

Command List

active (ping-polling)

Overview This command enables a ping-poll instance. The polling instance sends ICMP echo requests to the device with the IP address specified by the ip (ping-polling) command.

By default, polling instances are disabled. When a polling instance is enabled, it assumes that the device it is polling is unreachable.

The **no** variant of this command disables a ping-poll instance. The polling instance no longer sends ICMP echo requests to the polled device. This also resets all counters for this polling instance.

Syntax

```
active
no active
```

Mode Ping-Polling Configuration

Examples To activate the ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# active
```

To disable the ping-poll instance 43 and reset its counters, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no active
```

Related Commands

debug ping-poll

ip (ping-polling)

ping-poll

show ping-poll

clear ping-poll

Overview This command resets the specified ping poll, or all ping poll instances. This clears the ping counters, and changes the status of polled devices to unreachable. The polling instance changes to the polling frequency specified with the critical-interval command. The device status changes to reachable once the device responses have reached the up-count.

Syntax

```
clear ping-poll {<1-100>|all}
```

Parameter	Description
<1-100>	A ping poll ID number. The specified ping poll instance has its counters cleared, and the status of the device it polls is changed to unreachable.
`all`	Clears the counters and changes the device status of all polling instances.

Mode Privileged Exec

Examples To reset the ping poll instance 12, use the command:

```
awplus# clear ping-poll 12
```

To reset all ping poll instances, use the command:

```
awplus# clear ping-poll all
```

Related Commands

active (ping-polling)

ping-poll

show ping-poll

critical-interval

Overview This command specifies the time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable.

This command enables the device to quickly observe changes in state, and should be set to a much lower value than the normal-interval command.

The **no** variant of this command sets the critical interval to the default of one second.

Syntax

```
critical-interval <1-65536>
no critical-interval
```

Parameter	Description
<1-65536>	Time in seconds between pings, when the device has failed to a ping, or the device is unreachable.

Default The default is 1 second.

Mode Ping-Polling Configuration

Examples To set the critical interval to 2 seconds for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# critical-interval 2
```

To reset the critical interval to the default of one second for the ping-polling instance 99, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 99
awplus(config-ping-poll)# no critical-interval
```

Related Commands

fail-count

normal-interval

sample-size

show ping-poll

timeout (ping polling)

up-count

debug ping-poll

Overview This command enables ping poll debugging for the specified ping-poll instance. This generates detailed messages about ping execution.

The **no** variant of this command disables ping-poll debugging for the specified ping-poll.

Syntax

```
debug ping-poll <1-100>
no debug ping-poll {<1-100>|all}
```

Parameter	Description
<1-100>	A unique ping poll ID number.
all	Turn off all ping-poll debugging.

Mode Privileged Exec

Examples To enable debugging for ping-poll instance 88, use the command:

```
awplus# debug ping-poll 88
```

To disable all ping poll debugging, use the command:

```
awplus# no debug ping-poll all
```

To disable debugging for ping-poll instance 88, use the command:

```
awplus# no debug ping-poll 88
```

Related Commands

active (ping-polling)

clear ping-poll

ping-poll

show ping-poll

undebug ping-poll

description (ping-polling)

Overview This command specifies a string to describe the ping-polling instance. This allows the ping-polling instance to be recognized easily in show commands. Setting this command is optional.

By default ping-poll instances do not have a description.

Use the **no** variant of this command to delete the description set.

Syntax

```
description <description>
no description
```

Parameter	Description
<description>	The description of the target. Valid characters are any printable character and spaces. There is no maximum character length.

Mode Ping-Polling Configuration

Examples To add the text “Primary Gateway” to describe the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# description Primary Gateway
```

To delete the description set for the ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no description
```

Related Commands ping-poll

show ping-poll

fail-count

Overview This command specifies the number of pings that must be unanswered, within the total number of pings specified by the sample-size command, for the ping-polling instance to consider the device unreachable.

If the number set by the sample-size command and the **fail-count** commands are the same, then the unanswered pings must be consecutive. If the number set by the sample-size command is greater than the number set by the **fail-count** command, then a device that does not always reply to pings may be declared unreachable.

The **no** variant of this command resets the fail count to the default.

Syntax

```
fail-count <1-100>
no fail-count
```

Parameter	Description
<1-100>	The number of pings within the sample size that a reachable device must fail to respond to before it is classified as unreachable.

Default The default is 5.

Mode Ping-Polling Configuration

Examples To specify the number of pings that must fail within the sample size to determine that a device is unreachable for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# fail-count 5
```

To reset the fail-count to its default of 5 for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no fail-count
```

Related Commands

critical-interval

normal-interval

ping-poll

sample-size

show ping-poll

timeout (ping polling)

up-count

ip (ping-polling)

Overview This command specifies the IPv4 address of the device you are polling.

Syntax

```
ip {<ip-address>|<ipv6-address>}
```

Parameter	Description
<ip-address>	An IPv4 address in dotted decimal notation `A.B.C.D`
<ipv6-address>	An IPv6 address in hexadecimal notation `X:X::X:X`

Mode Ping-Polling Configuration

Examples To set ping-poll instance 5 to poll the device with the IP address `192.168.0.1`, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 5
awplus(config-ping-poll)# ip 192.168.0.1
```

To set ping-poll instance 10 to poll the device with the IPv6 address `2001:db8::`, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 10
awplus(config-ping-poll)# ip 2001:db8::
```

Related Commands

ping-poll

source-ip

show ping-poll

length (ping-poll data)

Overview This command specifies the number of data bytes to include in the data portion of the ping packet. This allows you to set the ping packets to a larger size if you find that larger packet types in your network are not reaching the polled device, while smaller packets are getting through. This encourages the polling instance to change the device's status to unreachable when the network is dropping packets of the size you are interested in.

The **no** variant of this command resets the data bytes to the default of 32 bytes.

Syntax

```
length <4-1500>
no length
```

Parameter	Description
<4-1500>	The number of data bytes to include in the data portion of the ping packet.

Default The default is 32.

Mode Ping-Polling Configuration

Examples To specify that ping-poll instance 12 sends ping packet with a data portion of 56 bytes, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length 56
```

To reset the number of data bytes in the ping packet to the default of 32 bytes for ping- poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 12
awplus(config-ping-poll)# length
```

Related Commands ping-poll

show ping-poll

normal-interval

Overview This command specifies the time period between pings when the device is reachable.

The **no** variant of this command resets the time period to the default of 30 seconds.

Syntax

```
normal-interval <1-65536>
no normal-interval
```

Parameter	Description
<1-65536>	Time in seconds between pings when the target is reachable.

Default The default is 30 seconds.

Mode Ping-Polling Configuration

Examples To specify a time period of 60 seconds between pings when the device is reachable for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# normal-interval 60
```

To reset the interval to the default of 30 seconds for ping-poll instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no normal-interval
```

Related Commands

critical-interval

fail-count

ping-poll

sample-size

show ping-poll

timeout (ping polling)

up-count

ping-poll

Overview This command enters the ping-poll configuration mode. If a ping-poll exists with the specified number, then this command enters its configuration mode. If no-ping poll exists with the specified number, then this command creates a new ping poll with this ID number.

To configure a ping-poll, create a ping poll using this command, and use the ip (ping-polling) command to specify the device you want the polling instance to poll. It is not necessary to specify any further commands unless you want to change a command's default.

The **no** variant of this command deletes the specified ping poll.

Syntax

```
ping-poll <1-100>
no ping-poll <1-100>
```

Parameter	Description
<1-100>	A unique ping poll ID number.

Mode Global Configuration

Examples To create ping-poll instance 3 and enter ping-poll configuration mode, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 3
awplus(config-ping-poll)#
```

To delete ping-poll instance 3, use the commands:

```
awplus# configure terminal
awplus(config)# no ping-poll 3
```

Related Commands

active (ping-polling)

clear ping-poll

debug ping-poll

description (ping-polling)

ip (ping-polling)

length (ping-poll data)

show ping-poll

source-ip

sample-size

Overview This command sets the total number of pings that the polling instance inspects when determining whether a device is unreachable. If the number of pings specified by the **fail-count** command go unanswered within the inspected sample, then the device is declared unreachable.

If the numbers set in this command and fail-count command are the same, the unanswered pings must be consecutive. If the number set by this command is greater than that set with the fail-count command, a device that does not always reply to pings may be declared unreachable.

You cannot set this command's value lower than the fail-count value.

The polling instance uses the number of pings specified by the up-count command to determine when a device is reachable.

The **no** variant of this command resets this command to the default.

Syntax

```
sample-size <1-100>
no sample size
```

Parameter	Description
<1-100>	Number of pings that determines critical and up counts.

Default The default is 5.

Mode Ping-Polling Configuration

Examples To set the sample-size to 50 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# sample-size 50
```

To reset sample-size to the default of 5 for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no sample-size
```

Related Commands

critical-interval

fail-count

normal-interval

ping-poll

show ping-poll

timeout (ping polling)

up-count

show counter ping-poll

Overview This command displays the counters for ping polling.

Syntax

```
show counter ping-poll [<1-100>]
```

Parameter	Description
<1-100>	A unique ping poll ID number. This displays the counters for the specified ping poll only. If you do not specify a ping poll, then this command displays counters for all ping polls.

Mode User Exec and Privileged Exec

Output Figure 50-1: Example output from the **show counter ping-poll** command

```
Ping-polling counters
Ping-poll: 1
PingsSent              ......... 15
PingsFailedUpState     ......... 0
PingsFailedDownState   ......... 0
ErrorSendingPing       ......... 2
CurrentUpCount         ......... 13
CurrentFailCount       ......... 0
UpStateEntered         ......... 0
DownStateEntered       ......... 0

Ping-poll: 2
PingsSent              ......... 15
PingsFailedUpState     ......... 0
PingsFailedDownState   ......... 0
ErrorSendingPing       ......... 2
CurrentUpCount         ......... 13
CurrentFailCount       ......... 0
UpStateEntered         ......... 0
DownStateEntered       ......... 0

Ping-poll: 5
PingsSent              ......... 13
PingsFailedUpState     ......... 0
PingsFailedDownState   ......... 2
ErrorSendingPing       ......... 2
CurrentUpCount         ......... 9
CurrentFailCount       ......... 0
UpStateEntered         ......... 0
DownStateEntered       ......... 0
```

Table 51: Parameters in output of the **show counter ping-poll** command

Parameter	Description
`Ping-poll`	The ID number of the polling instance.
`PingsSent`	The total number of pings generated by the polling instance.
`PingsFailedUpState`	The number of unanswered pings while the target device is in the Up state. This is a cumulative counter for multiple occurrences of the Up state.
`PingsFailedDownState`	Number of unanswered pings while the target device is in the Down state. This is a cumulative counter for multiple occurrences of the Down state.
`ErrorSendingPing`	The number of pings that were not successfully sent to the target device. This error can occur when your device does not have a route to the destination.
`CurrentUpCount`	The current number of sequential ping replies.
`CurrentFailCount`	The number of ping requests that have not received a ping reply in the current sample-size window.
`UpStateEntered`	Number of times the target device has entered the Up state.
`DownStateEntered`	Number of times the target device has entered the Down state.

Example To display counters for the polling instances, use the command:

```
awplus# show counter ping-poll
```

Related Commands

debug ping-poll

ping-poll

show ping-poll

show ping-poll

Overview This command displays the settings and status of ping polls.

Syntax `show ping-poll [<1-100>|state {up|down}] [brief]`

Parameter	Description	
<1-100>	Displays settings and status for the specified polling instance.	
`state`	Displays polling instances based on whether the device they are polling is currently reachable or unreachable.	
	`up`	Displays polling instance where the device state is reachable.
	`down`	Displays polling instances where the device state is unreachable.
`brief`	Displays a summary of the state of ping polls, and the devices they are polling.	

Mode User Exec and Privileged Exec

Output Figure 50-2: Example output from the **show ping-poll brief** command

```
Ping Poll Configuration
-------------------------------------------------------
Id Enabled State Destination
-------------------------------------------------------
1  Yes     Down  192.168.0.1
2  Yes     Up    192.168.0.100
```

Table 52: Parameters in output of the **show ping-poll brief** command

Parameter	Meaning
Id	The ID number of the polling instance, set when creating the polling instance with the ping-poll command.
Enabled	Whether the polling instance is enabled or disabled.

Table 52: Parameters in output of the **show ping-poll brief** command (cont.)

Parameter	Meaning	
State	The current status of the device being polled:	
	Up	The device is reachable.
	Down	The device is unreachable.
	Critical Up	The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.
	Critical Down	The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.
Destination	The IP address of the polled device, set with the ip (ping-polling) command.	

Figure 50-3: Example output from the **show ping-poll** command

```
Ping Poll Configuration
-------------------------------------------------------------

Poll 1:
Description                         : Primary Gateway
Destination IP address              : 192.168.0.1
Status                              : Down
Enabled                             : Yes
Source IP address                   : 192.168.0.10
Critical interval                   : 1
Normal interval                     : 30
Fail count                          : 10
Up count                            : 5
Sample size                         : 50
Length                              : 32
Timeout                             : 1
Debugging                           : Enabled
```

```
Poll 2:
Description                          : Secondary Gateway
Destination IP address               : 192.168.0.100
Status                               : Up
Enabled                              : Yes
Source IP address                    : Default
Critical interval                    : 5
Normal interval                      : 60
Fail count                           : 20
Up count                             : 30
Sample size                          : 100
Length                               : 56
Timeout                              : 2
Debugging                            : Enabled
```

Table 53: Parameters in output of the **show ping-poll** command

Parameter	Description	
Description	Optional description set for the polling instance with the description (ping-polling) command.	
Destination IP address	The IP address of the polled device, set with the ip (ping-polling) command.	
Status	The current status of the device being polled:	
	Up	The device is reachable.
	Down	The device is unreachable.
	Critical Up	The device is reachable but recently the polling instance has not received some ping replies, so the polled device may be going down.
	Critical Down	The device is unreachable but the polling instance received a reply to the last ping packet, so the polled device may be coming back up.
Enabled	Whether the polling instance is enabled or disabled. The active (ping-polling) and active (ping-polling) commands enable and disable a polling instance.	
Source IP address	The source IP address sent in the ping packets. This is set using the source-ip command.	
Critical interval	The time period in seconds between pings when the polling instance has not received a reply to at least one ping, and when the device is unreachable. This is set with the critical-interval command.	
Normal interval	The time period between pings when the device is reachable. This is set with the normal-interval command.	

Table 53: Parameters in output of the **show ping-poll** command (cont.)

Parameter	Description
`Fail count`	The number of pings that must be unanswered, within the total number of pings specified by the sample-size command, for the polling instance to consider the device unreachable. This is set using the fail-count command.
`Up count`	The number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again. This is set using the up-count command.
`Sample size`	The total number of pings that the polling instance inspects when determining whether a device is unreachable. This is set using the sample-size command.
`Length`	The number of data bytes to include in the data portion of the ping packet. This is set using the length (ping-poll data) command.
`Timeout`	The time in seconds that the polling instance waits for a response to a ping packet. This is set using the timeout (ping polling) command.
`Debugging`	Indicates whether ping polling debugging is **Enabled** or **Disabled**. This is set using the debug ping-poll command.

Examples

To display the ping poll settings and the status of all the polls, use the command:

```
awplus# show ping-poll
```

To display a summary of the ping poll settings, use the command:

```
awplus# show ping-poll brief
```

To display the settings for ping poll 6, use the command:

```
awplus# show ping-poll 6
```

To display a summary of the state of ping poll 6, use the command:

```
awplus# show ping-poll 6 brief
```

To display the settings of ping polls that have reachable devices, use the command:

```
awplus# show ping-poll state up
```

To display a summary of ping polls that have unreachable devices, use the command:

```
awplus# show ping-poll 6 state down brief
```

Related Commands

debug ping-poll

ping-poll

source-ip

Overview This command specifies the source IP address to use in ping packets.

By default, the polling instance uses the address of the interface through which it transmits the ping packets. It uses the device's local interface IP address when it is set. Otherwise, the IP address of the interface through which it transmits the ping packets is used.

The **no** variant of this command resets the source IP in the packets to the device's local interface IP address.

Syntax

```
source-ip {<ip-address>|<ipv6-address>}
no source-ip
```

Parameter	Description
<ip-address>	An IPv4 address in dotted decimal notation `A.B.C.D`
<ipv6-address>	An IPv6 address in hexadecimal notation `X:X::X:X`

Mode Ping-Polling Configuration

Examples To configure the ping-polling instance 43 to use the source IP address `192.168.0.1` in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 192.168.0.1
```

To configure the ping-polling instance 43 to use the source IPv6 address `2001:db8::` in ping packets, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# source-ip 2001:db8::
```

To reset the source IP address to the device's local interface IP address for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no source-ip
```

Related Commands

description (ping-polling)

ip (ping-polling)

length (ping-poll data)

ping-poll

show ping-poll

timeout (ping polling)

Overview This command specifies the time in seconds that the polling instance waits for a response to a ping packet. You may find a higher time-out useful in networks where ping packets have a low priority.

The **no** variant of this command resets the set time out to the default of one second.

Syntax

```
timeout <1-30>
no timeout
```

Parameter	Description
<1-30>	Length of time, in seconds, that the polling instance waits for a response from the polled device.

Default The default is 1 second.

Mode Ping-Polling Configuration

Examples To specify the timeout as 5 seconds for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# timeout 5
```

To reset the timeout to its default of 1 second for ping-poll instance 43, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 43
awplus(config-ping-poll)# no timeout
```

Related Commands

critical-interval

fail-count

normal-interval

ping-poll

sample-size

show ping-poll

up-count

up-count

Overview This command sets the number of consecutive pings that the polling instance must receive a reply to before classifying the device reachable again.

The **no** variant of this command resets the up count to the default of 30.

Syntax

```
up-count <1-100>
no up-count
```

Parameter	Description
<1-100>	Number of replied pings before an unreachable device is classified as reachable.

Default The default is 30.

Mode Ping-Polling Configuration

Examples To set the upcount to 5 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# up-count 5
```

To reset the upcount to the default value of 30 consecutive pings for ping-polling instance 45, use the commands:

```
awplus# configure terminal
awplus(config)# ping-poll 45
awplus(config-ping-poll)# no up-count
```

Related Commands

critical-interval

fail-count

normal-interval

ping-poll

sample-size

show ping-poll

timeout (ping polling)

undebug ping-poll

Overview This command applies the functionality of the no debug ping-poll command.

51 sFlow Commands

Introduction

Overview This chapter provides an alphabetical reference for sFlow commands.

Command List

debug sflow

Overview This command enables sFlow® debug message logging, for sFlow sampling and polling activity on the specified ports. If no ports are specified, sampling and/or polling debug messages are enabled for all ports.

The **no** variant of this command disables sFlow sampling and or polling debug message logging on the ports selected. If no ports are specified, sampling and/or polling debug messages are disabled on all ports.

Syntax

```
debug sflow [interface <port-list>] [sampling][polling]
no debug sflow [interface <port-list>] [sampling][polling]
```

Parameter	Description
`interface`	Interface information.
<port-list>	The ports for which sFlow debug is to be enabled. The ports to display information about. The port list can be: • a switch port (e.g. `port1.0.12`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.1-1.0.24`.
`sampling`	Debug sFlow sampling for the specified port(s).
`polling`	Debug sFlow polling for the specified port(s).

Default The sFlow sampling and or polling debug is disabled.

Mode Privileged Exec

Examples To enable sFlow debug message logging for polling and sampling on `port1.0.1` and `port1.0.7`, use the commands:

```
awplus# debug sflow interface port1.0.1,port1.0.7 sampling
polling
```

To enable logging and polling of sFlow debug messages for polling and sampling on all ports, use the command:

```
awplus# debug sflow sampling polling
```

Related Commands show debugging sflow

no debug all

debug sflow agent

Overview This command enables sFlow® debug message logging that is not specific to particular ports. For example, sending an sFlow datagram to the collector.

The **no** variant of this command applies the command default.

Syntax

```
debug sflow agent
no debug sflow agent
```

Default The sFlow agent debug message logging (that is not port specific) is disabled.

Mode Privileged Exec

Example To enable logging of sFlow agent debug messages, use the following command:

```
awplus# debug sflow agent
```

Related Commands show debugging sflow

debug sflow

sflow agent (address)

Overview This command sets the sFlow® agent IP address on the switch. This address is inserted into every sFlow datagram sent from the sFlow agent switch to the sFlow collector device. The sFlow collector can then uses this address to uniquely identify and to access the switch, such as for SNMP. We therefore recommend that you change this address as little as possible.

Although the agent address can be set to any valid IPv4 or IPv6 address; we recommended that you set the sFlow® agent IP address to be the **local address** that is configured on the switch. For information on local addresses and how to set them up, see the interface (to configure) command. This ensures that the sFlow collector can maintain connectivity to the switch irrespective of the addition or deletion of VLAN interfaces (each of which will have its own specific IP address). Note that sFlow is rendered inactive whenever the agent address is not set.

The **no** variant of this command applies its default setting to remove a configured address.

Syntax

```
sflow agent {ip <ip-address>|ipv6 <ipv6-address>}
no sflow agent {ip|ipv6}
```

Parameter	Description
<ip-address>	The IPv4 address of the switch that is acting as the sFlow agent.
<ipv6-address>	The IPv6 address of the switch that is acting as the sFlow agent. The IPv6 address uses the format X:X::X:X.

Default The sFlow agent address is unset.

Mode Global Configuration

Examples To set the sFlow agent (IPv4) address to `192.0.2.23`, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ip 192.0.2.23
```

To remove the sFlow agent (IPv4) address, use the command:

```
awplus# configure terminal
awplus(config)# no sflow agent ip
```

To set the sFlow agent (IPv6) address to `2001:0db8::1`, use the command:

```
awplus# configure terminal
awplus(config)# sflow agent ipv6 2001:0db8::1
```

To remove the sFlow agent (IPv6) address, use the command:

```
awplus# configure terminal
awplus(config)# no sflow agent ipv6
```

Related Commands

show running-config sflow

show sflow

sflow collector (address)

Overview This command sets the sFlow® agent's collector IP address and/or UDP port. This is the destination IP address and UDP port, for sFlow datagrams sent from the sFlow agent. The IP address can be any valid IPv4 or IPv6 address. Note that sFlow is rendered inactive whenever the collector address is set to 0.0.0.0 (for IPv4) or `::` (for IPv6).

The **no** variant of this command returns the IP address and UDP port values to their defaults, which will result in sFlow being deactivated.

Syntax

```
sflow collector {[ip <ip-address>|ipv6 <ipv6-address>]|[port <1-65535>]}
no sflow collector {[ip|ipv6]|[port]}
```

Parameter	Description
<ip-address>	IPv4 address of the remote sFlow collector.
<ipv6-address>	IPv6 address of remote sFlow collector. The IPv6 address uses the format X:X::X:X.
`port`	Destination UDP port for sFlow datagrams sent to the collector.
<1-65535>	UDP port number (default: 6343).

Default The collector address is `0.0.0.0` (which renders sFlow inactive), and the UDP port is `6343`.

Mode Global Configuration

Examples To set the sFlow collector address to `1920.2.25` and UDP port to `9000`, use the command:

```
awplus# configure terminal
awplus(config)# sflow collector ip 192.0.2.25 port 9000
```

To remove the sFlow collector IPv4 address and leave the UDP port unchanged, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ip
```

To remove the sFlow collector IPv4 address and to remove the UDP port, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ip port
```

To set the sFlow collector address to `2001:0db8::1` and leave the UDP port unchanged, use the command:

```
awplus# configure terminal
awplus(config)# sflow collector ipv6 2001:0db8::1
```

To remove the sFlow collector IPv6 address and leave the UDP port unchanged, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ipv6
```

To remove the sFlow collector IPv6 address and to remove the UDP port, use the command:

```
awplus# configure terminal
awplus(config)# no sflow collector ipv6 port
```

Related Commands

show running-config sflow

show sflow

sflow collector max-datagram-size

Overview This command sets the maximum size of the sFlow® datagrams sent to the collector.

The **no** variant of this command resets the maximum-datagram-size to the default.

Syntax

```
sflow collector max-datagram-size <200-1500>
no sflow collector max-datagram-size
```

Parameter	Description
<200-1500>	The maximum number of bytes that can be sent in an sFlow datagram sent from the agent to the collector.

Default 1400 bytes

Mode Global Configuration

Example To set the maximum datagram size to 1200, use the command:

```
awplus# configure terminal
awplus(config)# sflow collector max-datagram-size 1200
```

Related Commands

show running-config sflow

show sflow

sflow enable

Overview This command enables sFlow® globally on the switch.

The **no** variant of this command disables sFlow globally on the switch.

Note that enabling sFlow does not automatically set its operational status to active. To activate sFlow the following conditions need to be met:

- sFlow is enabled.
- The sFlow agent address is set.
- The sFlow collector address is set to a valid (non zero) IPv4 or IPv6 address.
- Polling or sampling is enabled on the ports to be sampled or polled.

Syntax

```
sflow enable
no sflow enable
```

Default sFlow is disabled globally on the switch.

Mode Global Configuration

Example To enable sFlow operation, use the command:

```
awplus# configure terminal
awplus(config)# sflow enable
```

Related Commands show running-config sflow

show sflow

sflow max-header-size

Overview This command sets the maximum header size of the Ethernet frames sampled on a specified port. The maximum header size is measured in bytes, referenced from the first byte of the Ethernet destination address and excludes the Ethernet FCS fields.

If a sampled Ethernet frame is longer than the maximum header size set by this command, then the frame will be truncated to the first N bytes before being placed in the sFlow datagram, where N is the maximum header size set by this command.

The **no** variant of this command resets the max-header-size to its default.

Syntax

```
sflow max-header-size <14-200>
no sflow max-header-size
```

Parameter	Description
<14-200>	The maximum number of header bytes to be sampled.

Default The max-header-size is 128 bytes.

Mode Interface Configuration

Usage The header size is measured from the first byte of the Ethernet frame MAC Destination Address.

- For an environment using standard TCP IPv4 over Ethernet frames, consider the following basic protocol structure:

  Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes

  IPv4 header = 24 bytes

  TCP header = 24 bytes

  Total = 66 bytes

  CAUTION: *For IPv4, any data existing between 66 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-66=62 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.*

  For more information, see the sFlow Feature Overview and Configuration Guide.

- A similar consideration can be made for an environment using TCP IPv6 over Ethernet:

  Ethernet header (including the 4 byte 802.1Q header component) = 18 bytes

  IPv6 header = 40 bytes

  TCP header = 24 bytes

  Total = 82 bytes

  CAUTION: *For IPv6, any data existing between 82 bytes and the value set by this command will be included in the sFlow packet samples. For example, with the default of 128 applied, up to 128-82=46 bytes of user data could be included in the sFlow datagram samples sent between the Agent and the Collector.*

Note that the agent-to-collector datagrams contain their own UDP headers, which are outside this calculation.

Example To set the maximum header size to 160 bytes for ports 1.0.1 and 1.0.7, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.7
awplus(config-if)# sflow max-header-size 160
```

Related Commands

show running-config sflow

show sflow interface

sflow max-header-size

sflow polling-interval

Overview This command sets the sFlow® counter polling interval (in seconds) for the specified ports. A value of 0 disables polling. A counter sample is taken every N seconds where N is the value set by this command.

The **no** variant of this command applies the default.

Syntax

```
sflow polling-interval {0|<1-16777215>}
no sflow polling-interval
```

Parameter	Description
0	Disable polling (the default).
<1-16777215>	The polling interval in seconds.

Default The polling-interval is 0 (polling disabled).

Mode Interface Configuration

Example To set the polling interval to 60 seconds for ports 1.0.1 and 1.0.7, use the following commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.7
awplus(config-if)# sflow polling-interval 60
```

Related Commands show running-config sflow

show sflow interface

sflow sampling-rate

Overview This command sets the mean sFlow® sampling rate for the specified ports. Sampling occurs every N frames (on average), where N is the rate value set via this command. The sampling rate applies to ingress and egress frames independently. For example, a value of 1000 will sample one frame in every 1000 frames received, i.e. one in every 1000 frames sent from the specified port. A value of 0 disables sampling on the specified port(s).

The **no** variant of this command applies the default.

Syntax

```
sflow sampling-rate {0|<256-16777215>}
no sflow sampling-rate
```

Parameter	Description
0	Sets the default.
<256-16777215>	The sampling rate N, measured in Ethernet frames.

Default The sampling-rate is 0 (sampling disabled).

Mode Interface Configuration

Example To set the sampling rate to 500 for ports 1.0.1 and 1.0.7, use the commands:

```
awplus# configure terminal
awplus(config)# interface port1.0.1,port1.0.7
awplus(config-if)# sflow sampling-rate 500
```

Related Commands

show running-config sflow

show sflow interface

show debugging sflow

Overview This command displays sFlow® debug settings for agent operation, and for sampling and polling on specific interface ports. If no interface ports are specified, sampling and polling will be applied to all ports.

Syntax

```
show debugging sflow [interface <port-list>]
```

Parameter	Description
`interface`	The interface information.
`<port-list>`	The ports for which the sFlow debug settings are to be shown. The ports to display information about. The port list can be: • a switch port (e.g. `port1.1.12`) • a continuous range of ports separated by a hyphen, e.g. `port1.0.1-1.0.24` • a comma-separated list of ports and port ranges, e.g. `port1.0.1,port1.0.1-1.0.24`.

Mode User Exec and Privileged Exec

Example To display sFlow debug settings on the agent, and for sampling and polling on ports 1.0.1 to 1.0.9, use the command:

```
awplus# show debugging sflow interface port1.0.1-1.0.9
```

Output Figure 51-1: Sample obtained for an sFlow agent

```
awplus# show debugging sflow interface port1.0.1-1.0.9

sFlow Agent Debug:    Enabled

          Sampling      Polling
Port       Debug         Debug
-------------------------------
1.0.1     Enabled       Enabled
1.0.2     Enabled          -
1.0.3        -             -
1.0.4        -             -
1.0.5        -             -
1.0.6        -          Enabled
1.0.7        -             -
1.0.8        -          Enabled
1.0.9        -          Enabled
```

To display sFlow debug settings for all ports, use the command:

```
awplus# show debugging sflow
```

Related Commands

show running-config sflow

show sflow interface

show running-config sflow

Overview This command displays the running system information specific to the sFlow feature.

Syntax
```
show running-config sflow
```

Mode Privileged Exec and Global Configuration

Example To display the sFlow running configuration information, use the command:

```
awplus# show running-config sflow
```

Output Figure 51-2: Example output from the **show running-config sflow** command

```
awplus#sh run sflow
!
sflow agent ip 192.0.2.33
sflow collector ip 192.0.2.65
sflow collector max-datagram-size 1200
sflow enable
!
interface port1.0.11-port1.0.22
 sflow sampling-rate 512
```

Related Commands show running-config

show sflow

Overview This command displays non-port-specific sFlow agent configuration and operational status.

Syntax

```
show sflow
```

Mode Privileged Exec

Example To display sFlow configuration and operational status, use the command:

```
awplus#  show sflow
```

Output

Table 1: Example output from the **show sflow** command

```
sFlow Agent Configuration:                    Default Values
  sFlow Admin Status ........ Disabled        [Disabled]
  sFlow Agent Address ....... [not set]       [not set]
  Collector Address ......... 0.0.0.0         [0.0.0.0]
  Collector UDP Port ........ 6343            [6343]
  Tx Max Datagram Size ...... 1200            [1400]

sFlow Agent Status:
  Polling/sampling/Tx ....... Inactive because:
                                - sFlow is disabled
                                - Agent Addr is not set
                                - Collector Addr is 0.0.0.0
                                - Polling & sampling disabled
                                  on all ports
```

Table 2: Parameters in the output of the **show sflow** command

Output Parameter	Description
sFlow Admin Status	Whether sFlow agent operation is administratively enabled.
sFlow Agent Address	The sFlow agent IPv4 or IPv6 address for the device. sFlow is rendered inactive whenever the agent address is not set.
Collector Address	The IPv4 or IPv6 collector address to which sFlow datagrams are sent. sFlow is rendered inactive whenever the collector address is set to 0.0.0.0 or 0:0::0.0.
Collector UDP Port	The UDP port on the collector to which sFlow datagrams are sent.

Table 2: Parameters in the output of the **show sflow** command (cont.)

Output Parameter	Description
`Tx Max Datagram Size`	The maximum size of the sFlow datagrams sent to the collector.
`Polling/sampling/ Tx`	Whether sFlow sampling and/or polling (and hence sFlow datagram transmission) are active. If inactive the reasons are listed.

Related Commands

show running-config sflow

show sflow interface

show sflow interface

Overview This command displays sFlow agent sampling and polling configuration for specified ports.

Syntax

```
show sflow interface <ifrange>
```

Parameter	Description
<ifrange>	The interface range.

Mode Privileged Exec

undebug sflow

Overview This command applies the functionality of the **no** variant of the debug sflow command.