Technical Guide

Getting Started with the AlliedWare Plus Command Line Interface

Introduction

This guide introduces a number of commonly-used management features of the AlliedWare Plus™ Operating System (OS).

Products and software version that apply to this guide

This guide applies to all AlliedWare Plus products, running version 5.4.4 or later.

However, feature support and implementation varies between products. For more information, see the following documents:

- The product's Installation Guide
- The product's Datasheet
- The product's Command Reference

These documents are available from the above links on our website at alliedtelesis.com.

Most of this guide applies for versions 5.4.4 onwards, but automatic IP address assignment on start-up applies from version 5.4.7-0.4 onwards.

Privacy Policy

As part of the normal functioning for providing network service, your device will store MAC and IP address information in both forwarding tables and as part of persistent logs of network events. In addition, a device may retain email addresses and user credentials as part of providing VPN services.

This information is available to device administrators but is not shared externally or retained beyond the life of the service. The device does not retain sufficient information to link such network identifiers to natural persons.

The only information visible to Allied Telesis servers relates to the identity of the device itself such as part of the AOC (Allied One Connect - Onboarding) service, or version data (e.g. as part of automated firmware updates).

Contents

Start-up process

From software version 5.4.7-0.4 onwards, unconfigured devices automatically receive a management IP address on start-up. When your device is started without any configuration, IPv4 and IPv6 addresses are automatically applied to the Ethernet-based management interface.

Your device must be factory new or unconfigured for automatic address assignment to occur. This means you can use SSH to manage your device remotely instead of locally.

Unconfigured (factory-new)

If your device is factory new it is considered unconfigured because none of the following configuration files exist in the root directory of external media:

- .config
- .config_backup
- .cfg files
- User created folders

Configured

Otherwise your device is considered configured. Your device may have an existing configuration or it could have been pre-configured (for example, Firewalls are pre-configured). You can use the command **erase factory-default** if you want to manually return it to an unconfigured state, so that automatic address assignment can occur.

For more information about erasing the factory default, see **How to return to the factory defaults**.

Management interfaces

The management interface depends on the interface ports available on your device.

Table 1: Management Interfaces

SWITCH	SWITCH OR FIREWALL	FIREWALL WITH NO SWITCHPORTS
eth0 labelled NET MGMT	vlan1 if there is no NET MGMT	The first eth port to go link-up

How the start-up process works

The following sequence of events occur after the management interface comes up on a factory-new (unconfigured) device:

- Nothing happens until the management interface goes link-up.
- If the management interface is vlan1, then your device waits until vlan1 has gone into a STP forwarding state.
- Telnet is automatically disabled and the SSH server is enabled.
- Loop Protection is enabled on devices that support it. Some devices (e.g. AR-Series Firewalls) do not support Loop Protection, so will not include the loop-protection configuration.
- DHCP and DHCPv6 clients are enabled and their processes started.
- An IPv6 link-local address is automatically assigned.
- If your device obtains an address from DHCP or DHCPv6, then the IP address is assigned.
- If your device does not obtain an IPv4 address via DHCP within 10 seconds, then it applies the class B IPv4 link-local address 169.254.42.42/16. Then the IPv4 DHCP client is disabled.

You can manage your device by using SSH to connect to the IPv4 or IPv6 address that has been assigned to the management interface. You will need to ensure your management computer is configured with an IP/IPv6 address within the same subnet as the management IP address on the device. The following commands are configured:

```
no service telnet
service ssh
ssh server allow-users manager
loop-protection loop-detect fast-block ldf-interval 1
interface <management-interface>
ip address dhcp
ipv6 address dhcp
```

Automatic IP address assignment

On new switches, an IP address is assigned automatically on start-up by either:

- a DHCP server
- if no DHCP server is available then the IP address 169.254.42.42 is assigned.

On new firewalls, the IP address 192.168.1.1 is assigned on vlan1.

How to login

You can choose one of the following options to login to your device:

- **Login from the console port**

  Use the console to login to your device if you have cable access via the local Console Port.

- **Login to a management interface port with SSH**

  Use SSH to login to your device via a Management Interface Port if you do not have access via the Console Port, or if you want to manage your device remotely.

- **Login with the web-based firewall GUI**

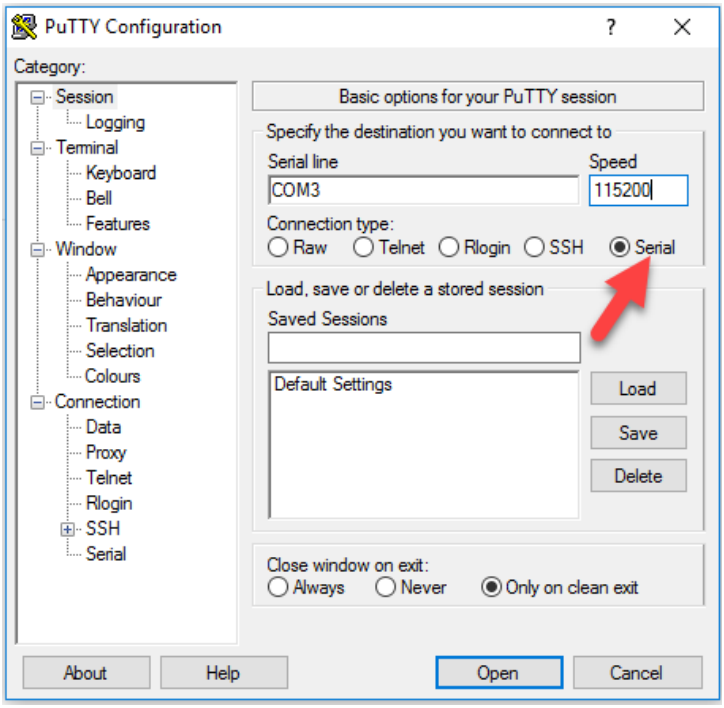
  Use the firewall GUI if you want to manage your device using web access.

Login from the console port

Follow these steps to login locally or out-of-band:

1. Connect the local management cable (with DB-9 connector) provided from your device to the management computer.
2. Power up your device (allow 10 seconds).
3. Open a PuTTY session (or equivalent terminal emulator).

   From the PuTTY Configuration dialog enter the following basic options:



   - Select the **Serial** button.
   - Enter the **Serial line**, for example COM3. To find the Serial line from Microsoft Windows, go to Device Manager> Ports (COM @ LPT).

- Change the **Speed** (console baud rate) if necessary, for example to 115200. The default baud rate is 9600. See your product's Installation Guide for the correct baud rate.

Caution

On IE200 and IE300 Series switches, we do not recommend changing the baud rate. The bootloader on these switches always runs at 9600 Baud. If you change the baud rate, you will lose access to the bootloader.

Click **Open** to establish a local management session with your device.

- Press **Enter** to display the login prompt.

  By default the AlliedWare Plus OS supports VT100 compatible terminals on the console port. This means that the terminal size is 80 columns by 24 rows.

4. Log in. The defaults are:

   - Username: **manager**
   - Password: **friend**

   Your device logs you into User Exec mode. From User Exec mode, you can perform high-level diagnostics (some **show** commands, ping, traceroute, for example), start sessions (Telnet, SSH), and change mode.

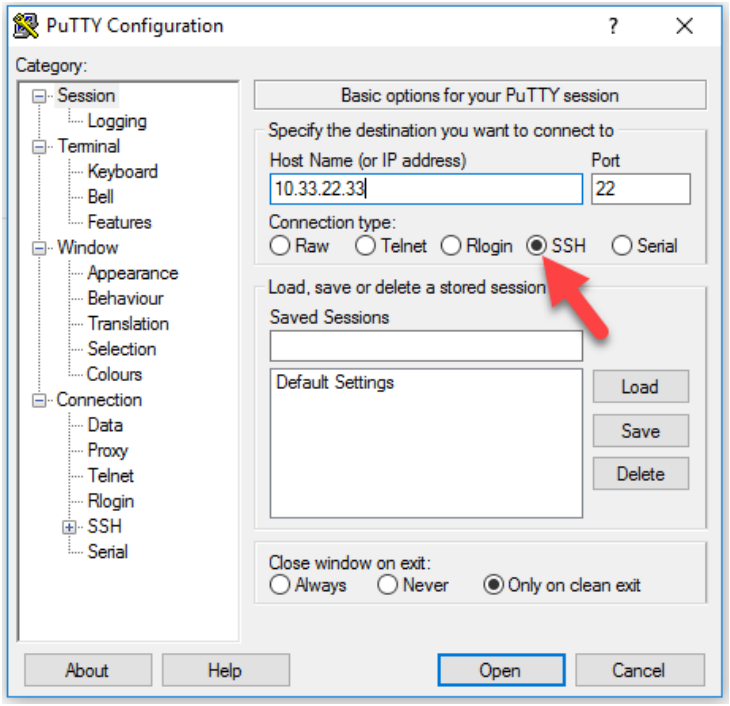
   You will be prompted to change the login password when you first log into a device that is in factory new state (or a device that has been reset to that state).

Login to a management interface port with SSH

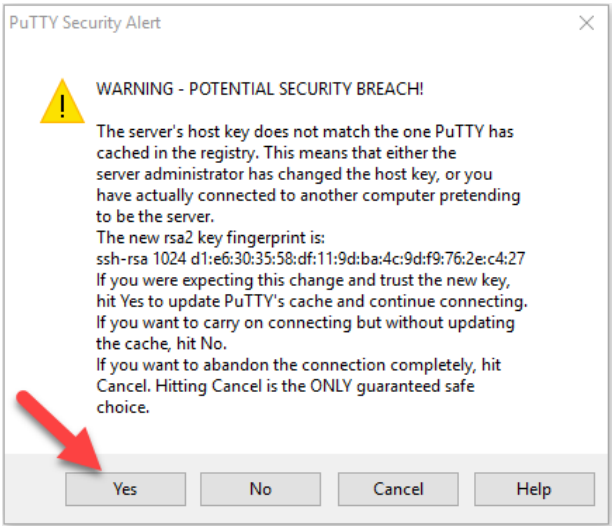
Follow these steps to login remotely to a management interface:

1. The management computer must have an IP address in the target subnet.
2. The management computer must be connected to the same network as the device.
3. Connect your device into the network via the management interface.
4. Power up your device. If your device is factory new (unconfigured) and you want it to receive an IP address automatically, wait approximately 30 seconds after the management port has gone link-up for this to happen. For details see **Automatic IP address assignment**.
5. Open a remote PuTTY session (or equivalent terminal emulator).

   From the PuTTY Configuration dialog enter the following basic options:



- Select the **SSH** button and enter the **Host Name (or IP address)**, for example 10.33.22.33.
- Click **Open** to establish a remote management session with your device.
- Click **Yes** if you receive the following PuTTY Security Alert Warning message:



This message can be bypassed because it is referring to the host key not matching the cache.

- Press **Enter** to display the login prompt.

  By default the AlliedWare Plus OS terminal size is 80 columns by 24 rows.

Login with the web-based firewall GUI

The firewall GUI provides setup of the firewall, enabling the configuration of entities (zones, networks and hosts) and then creating firewall, NAT, and traffic-control rules for managing traffic between these entities. Features such as the Intrusion Prevention System (IPS) and URL Filtering help protect the network, and manage website access.

The GUI also supports a DHCP server, interface management, VLAN management, file management, system tools, a CLI window and a dashboard for network monitoring. The dashboard shows interface and firewall traffic, system and environmental information, and the security monitoring widget lets you view and manage rules and security features. The complete AlliedWare Plus feature-set can be configured using the firewalls built-in industry standard Command Line Interface (CLI). The firewall and its graphical management and monitoring functionality will increase with subsequent releases.

If your firewall is new and unused, it will already have the GUI installed from the factory, and the IP address 192.168.1.1 on vlan1 and the HTTP service enabled. Connect to any switch port and browse to 192.168.1.1 to begin.

For further information about using the firewall GUI, see:

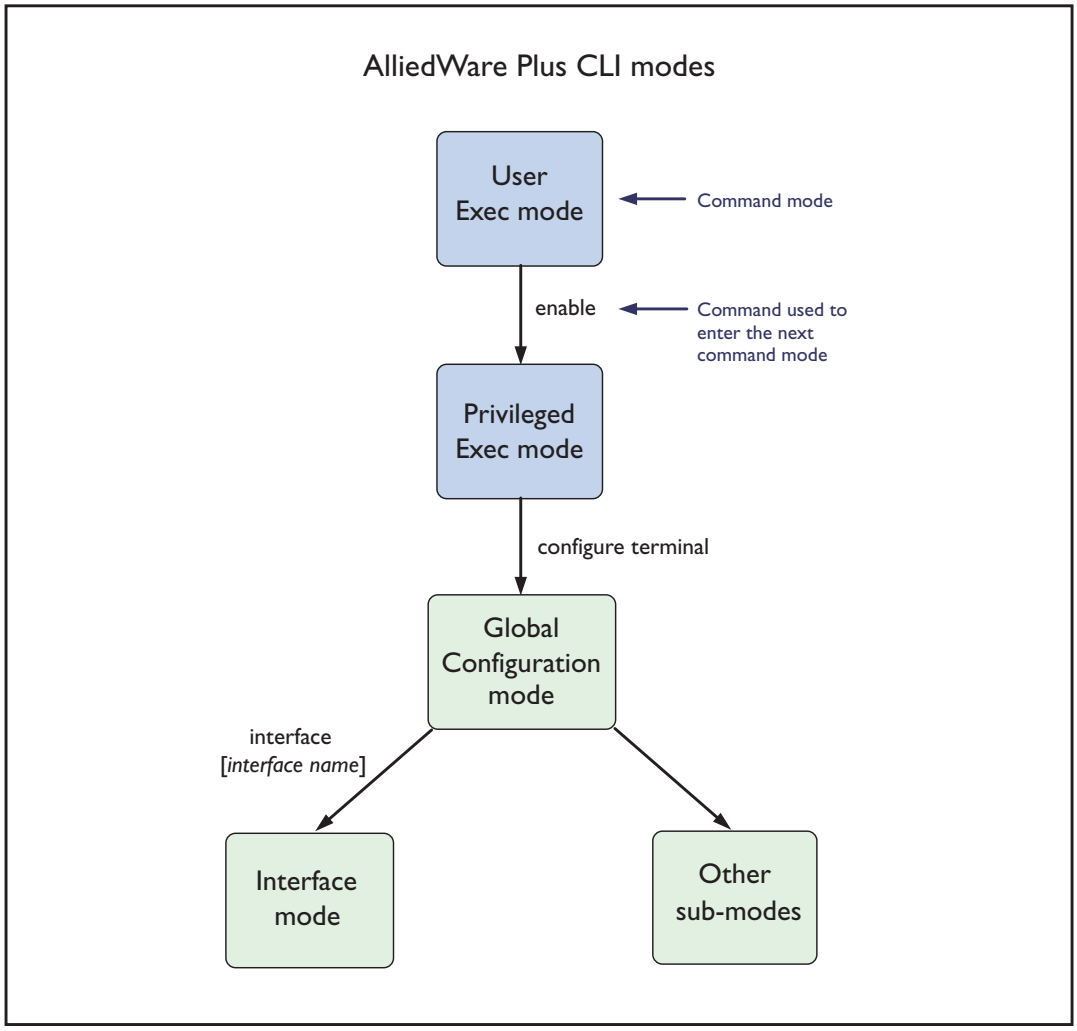
- Getting Started with the Device GUI on VPN Routers or
- Getting Started with the Device GUI on UTM Firewalls

How to work with command modes

AlliedWare Plus is modal, which means that the command line forms a hierarchy with different commands available at different levels of the hierarchy. Figure 1 below shows the command mode hierarchy and the commands you use to move to lower-level modes.

Multiple users can Telnet/SSH and issue commands using the User Exec mode and the Privileged Exec mode. However, only one user is allowed to use the Configuration mode at a time. This prevents multiple users from issuing configuration commands simultaneously.

Figure 1: AlliedWare Plus CLI modes



User Exec mode

User Exec mode is the mode you log into on the device. It lets you perform high-level diagnostics (**show** commands, ping, traceroute, for example), start sessions (Telnet, SSH), and change mode.

The default User Exec mode prompt is **awplus>**

Privileged Exec mode

Privileged Exec mode is the main mode for monitoring—for example, running **show** commands and debugging. From Privileged Exec mode, you can do all the commands from User Exec mode plus many system commands.

To change from User Exec to Privileged Exec mode, enter the command:

```
awplus> enable
```

The default Privileged Exec mode prompt is **awplus#**

Global Config mode

From Global Configuration mode, you can configure most aspects of the device.

To change from Privileged Exec to Global Configuration mode, enter the command:

```
awplus# configure terminal
```

The default Global Configuration mode prompt is **awplus(config)#**

Interface Config mode

From Interface Configuration mode, you can configure the settings of one or more specified interfaces.

To change from Global Configuration mode to Interface Configuration mode, enter the command:

```
awplus(config)# interface <interface-list>
```

<interface-list> is the name of one or more interfaces (for example, port1.0.1-1.0.3)

The default Interface Configuration mode prompt is **awplus(config-if)#**

Router Config mode

From Router Configuration mode, you can configure routing using BGP, IP, IPv6, OSPF, RIP, or VRRP.

To change from Global Configuration mode to Router Configuration mode, enter the command:

```
awplus(config)# router <protocol> <other-parameters>
```

The default Router Configuration mode prompt is **awplus(config-router)#**

VLAN Database mode

From VLAN Database mode, you can create and configure VLANs.

To change from Global Configuration mode to VLAN Database mode, enter the command:

```
awplus(config)# vlan database
```

The default VLAN Database mode prompt is **awplus(config-vlan)#**

Other lower-level configuration modes

A number of other features are also configured by entering a lower-level mode from Global Configuration mode.

The following tables lists some (but not all) examples of the lower-level modes:

MODE	WHAT IT CONFIGURES	COMMAND	DEFAULT PROMPT
Class map	QoS classes, which isolate and name specific traffic flows (classes) from all other traffic.	(first enable QoS globally with mls qos enable) class-map ***name***	`awplus(config-cmap)#`
EPSR	Ethernet Protection Switching Ring, a loop protection mechanism with extremely fast convergence times.	epsr configuration	`awplus(config-epsr)#`
Line	Console port settings or virtual terminal settings for Telnet.	line console 0 line vty ***number***	`awplus(config-line)#`
Ping poll	Ping polling, which checks whether specified devices are reachable or not.	ping-poll ***number***	`awplus(config-ping-poll)#`
Policy map	QoS policies, a collection of user-defined QoS classes and the default class.	(first enable QoS globally with mls qos enable) policy-map ***name***	`awplus(config-pmap)#`
Policy map class	The QoS actions to take on a class-map, and which class-maps to associate with a QoS policy. This mode is a sub-mode of Policy map mode.	(in Policy map mode) class ***name***	`awplus(config-pmap-c)#`
Route map	Route maps, which select routes to include or exclude from the device's routing table and/or route advertisements.	route-map ***name*** deny|permit ***entry-number***	`awplus(config-route-map)#`
MST	Multiple Spanning Tree Protocol.	spanning-tree mst configuration	`awplus(config-mst)#`
Trigger	Triggers, which run configuration scripts in response to events.	trigger ***number***	`awplus(config-trigger)#`

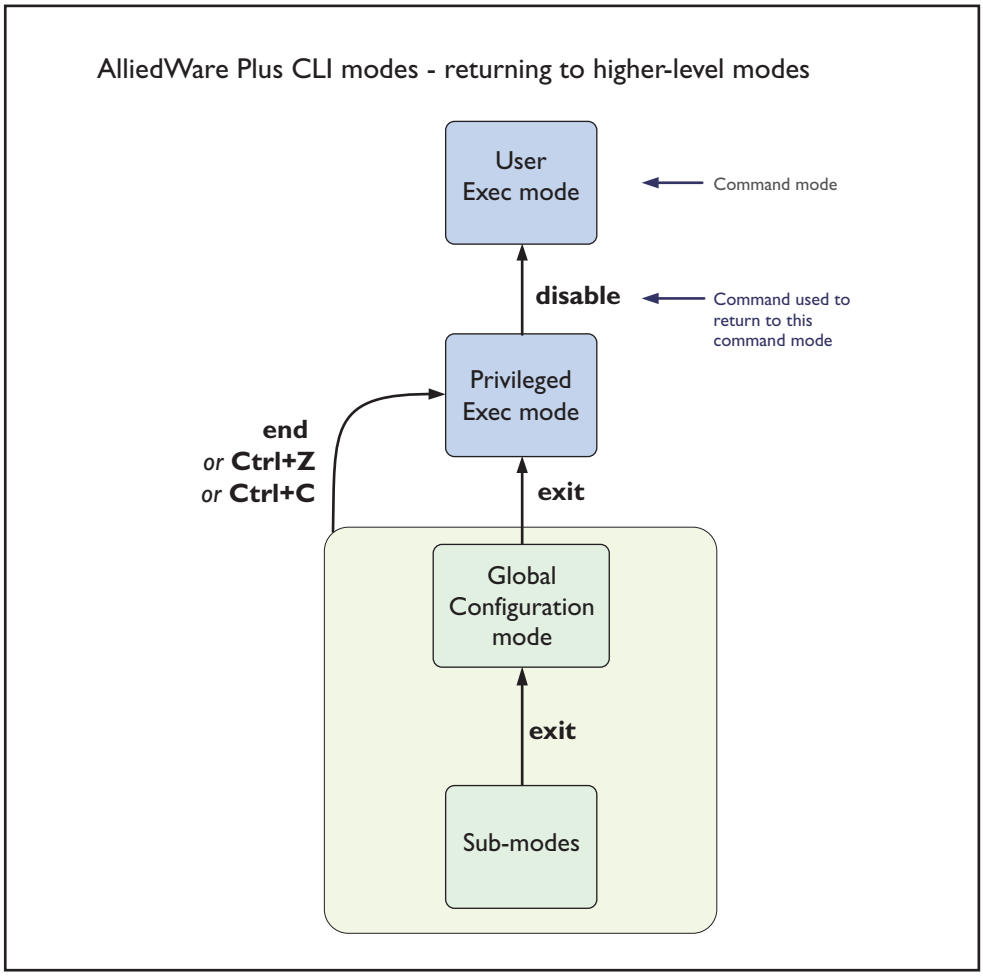
Some protocols have commands in both Global Configuration mode and lower-level configuration modes. For example, to configure MSTP, you use:

- Global Configuration mode to select MSTP as the spanning tree mode
- MST mode to create instances and specify other MSTP settings
- Interface Configuration mode to associate the instances with the appropriate ports.

Returning to higher-level modes

The following figure shows the commands to use to move from a lower-level mode to a higher-level mode.

Figure 2: Returning to higher-level modes



Examples To go from Interface Configuration to Global Configuration mode:

```
awplus(config-if)# exit
awplus(config)#
```

To go from Interface Configuration to Privileged Exec mode:

```
awplus(config-if)# end
awplus#
```

To go from Privileged Exec to User Exec:

```
awplus# exit
awplus>
```

Entering privileged exec commands when in a configuration mode

As you configure the device you will be constantly entering various **show** commands to confirm your configuration. This requires constantly changing between configuration modes and Privileged Exec mode.

However, you can run Privileged Exec commands without changing mode, by using the command:

```
awplus(config)# do <command you want to run>
```

You cannot use the ? help to find out command syntax when using the **do** command.

Example To display information about the IP interfaces when in Global Configuration mode, enter the command:

```
awplus(config)# do show ip int brief
```

This results in the following output:

```
Interface          IP-Address       Status         Protocol
eth0               172.28.8.200     admin up       running
vlan1              unassigned       admin up       running
...
```

How to get command help

The following kinds of command help are available:

- lists of valid parameters with brief descriptions (the ? key)
- completion of keywords (the Tab key)
- error messages for incomplete or incorrect syntax

Command abbreviations

The AlliedWare Plus CLI contains a number of abbreviations for its commands.

For example, the **show interface** command can be entered in the abbreviated form shown below:

```
awplus# sh in vlan100
```

Viewing a list of valid parameters

To get syntax help, type **?** (i.e. “space question mark”) after:

- **the prompt**:

  this will list all commands available in the mode you are in.

- **one or more parameters**:

  this will list parameters that can come next in the partial command.

- **one or more letters of a parameter**:

  this will list matching parameters.

Note: The AlliedWare Plus OS only displays one screenful of text at a time, with the prompt “--More--” at the end of each screenful. Press the space bar to display the next screenful or the **Q** key to return to the command prompt.

Example To see which commands are available in Privileged Exec mode, enter “?” at the Privileged Exec mode command prompt:

```
awplus# ?
```

This results in the following output:

```
Exec commands:
activate        Activate a script
cd              Change the current working directory
clear           Reset functions
clock           Manage clock
configure       Enter configuration mode
copy            Copy from one file to another
...
```

Example To see which **show** commands that start with "i" are available in Privileged Exec mode, enter "?" after **show i**:

```
awplus# show i?
```

This results in the following output:

```
  interface          Select an interface to configure
  ip                 Internet Protocol (IP)
  ipv6               Internet Protocol version 6 (IPv6)
```

Examples To use the **?** help to work out the syntax for the **clock timezone** command, enter the following sequence of commands:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock ?
```

```
  summer-time  Manage summer-time
  timezone     Set clock timezone
```

```
awplus(config)# clock timezone ?
```

```
  TIMEZONE  Timezone name, up to 5 characters
```

```
awplus(config)# clock timezone NZST ?
```

```
  minus  negative offset
  plus   positive offset
```

```
awplus(config)# clock timezone NZST plus ?
```

```
  <0-12>  Time zone offset to UTC
```

```
awplus(config)# clock timezone NZST plus 12
```

The above example demonstrates that the **?** help only indicates what you can type **next**. For commands that have a series of parameters, like **clock timezone**, the **?** help does not make the number of parameters obvious.

Completing keywords

To complete keywords, type the **Tab** key after part of the command.

If only one keyword matches the partial command, the AlliedWare Plus OS fills in that keyword. If multiple keywords match, it lists them.

Examples In this example we use Tab completion in successive steps to build the complete command **show ip dhcp snooping**. We have included "<Tab>" to show where to type the Tab key — this is not displayed on screen.

```
awplus#show ip <Tab>
access-list  dhcp         dhcp-relay   domain-list  domain-name  filter
forwarding   igmp         interface    mroute       name-server  prefix-list
route        rpf          rrp          sockets      source       traffic
```

```
awplus#show ip d<Tab>
dhcp         dhcp-relay       domain-list      domain-name
```

```
awplus#show ip dhcp <Tab>
binding   pool      server    snooping
```

```
awplus#show ip dhcp s<Tab>
server    snooping
```

Viewing command error messages

The device displays the following generic error messages about command input:

% Incomplete command—this message indicates that the command requires more parameters. Use the ? help to find out what other parameters are available.

```
awplus# interface
```

```
% Incomplete command.
```

% Invalid input detected at '^' marker—this indicates that the device could not process the command you entered. The device also prints the command and marks the first invalid character by putting a '^' under it. Note that you may get this error if you enter a command in the wrong mode, as the following output shows.

```
awplus# interface port1.0.1
```

```
interface port1.0.1
 ^
% Invalid input detected at '^' marker.
```

% Unrecognized command—when you try to use ? help and get this message, it indicates that the device can not provide help on the command because it does not recognize it. This means the command does not exist, or that you have entered it in the wrong mode, as the following output shows.

```
awplus# interface ?
```

```
% Unrecognized command
```

Note: The AlliedWare Plus OS does not tell you when commands are successful. If it does not display an error message, you can assume the command was successful.

How to see and change the running configuration

How to see the current configuration

The current configuration is called the **running-config**. To see it, enter the following command in either Privileged Exec mode or any configuration mode:

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

To see only part of the current configuration, enter the command:

```
awplus# show running-config|include <word>
```

This displays only the lines that contain ***word***.

To start the display at a particular place, enter the command:

```
awplus# show running-config|begin <word>
```

This searches the running-config for the first instance of ***word*** and begins the display from that line.

Note: The **show running-config** command works in all modes except User Exec mode.

Default settings

When the device initially started up with the AlliedWare Plus OS, it applied default settings and copied these defaults dynamically into its running-config.

These default settings mean that the AlliedWare Plus OS:

- encrypts passwords, such as user passwords.
- records log message priority in log messages.
- turns on jumbo frame support for all ports on devices with the **jumboframe** command.
- SSH is enabled.
- Telnet server is disabled by default.
- enables the device to look up domain names (but for domain name lookups to work, you have to configure a DNS server).
- turns off Layer 3 multicast packet switching in the switch's hardware (on Layer 3 switches). This prevents Layer 3 multicast from flooding the switch's CPU in its default state as a Layer 2 switch.
- sets the maximum number of ECMP routes, on devices that support ECMP.
- turns on RSTP on all ports. Note that the ports are not set to be edge ports.
- sets all the switch ports to access mode. This means they are untagged ports, suitable for connecting to hosts.
- creates VLAN 1 and adds all the switch ports to it.

- allows logins on the serial console port.
- allows logins on VTY sessions (for SSH, for example).
- forwards Layer 2 traffic appropriately without further configuration.
- allocates all the routing table memory space to IPv4 and IPv6 routes on devices that support IPv6 routing.
- allows configured ports to autonegotiate their speed and duplex mode.
- allows copper ports to be set to auto MDI/MDI-X mode.

The default configuration

Most of the above default settings are in the form of commands, which the device copied to its running-config when it first booted up.

For more information about start-up files, see "How to save and boot from the current configuration" on page 24. An example default configuration, with explanations of the meanings of the commands, is shown below:

CONTENTS OF DEFAULT SETTINGS	DESCRIPTION
`!`	An empty comment line (comments begin with an exclamation !).
`service password-encryption` `!`	Forces passwords in the script to be encrypted.
`no banner motd` `!`	No message of the day is set by default.
`log record-priority` `!`	Records log message priority.
`username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0`	Specifies the password for the manager user.
`ssh server allow-users manager`	The SSH server is set to allow the user manager.
`service ssh` `!`	SSH is enabled by default.
`no service telnet` `!`	Telnet is disabled by default.
`no clock timezone` `!`	The clock is disabled by default.

`snmp-server`
`!`
`!`
	SNMP is enabled by default.

`aaa authentication enable default local`	AAA authentication is enabled by default.
`aaa authentication login default local`	
`ip domain-lookup` `!`	Allows domain name lookups.
`no service dhcp-server` `!`	DHCP is disabled by default.

CONTENTS OF DEFAULT SETTINGS	DESCRIPTION
`no ip multicast-routing` `!`	Turns off L3 multicast packet switching in the switch hardware.
`spanning-tree mode rstp` `!`	Turns on RSTP.
`lacp global-passive-mode enable` `!`	LACP is enabled by default.
`interface eth0` `!`	A heading for any configuration settings for the management eth0 port. There are no eth0 settings.
`ip address dhcp` `ipv6 address dhcp`	The DHCP client is activated for IPv4 and IPv6. If DHCP fails, an address will be assigned as follows: ■ 169.254.42.42/16 for switches ■ 192.168.1.1 for routers, firewalls and access points.

`interface port1.0.1-1.0.24`
`switchport`
`switchport mode access`
`!`
	Sets each switch port to access mode.

`interface vlan1` `!`	Creates VLAN 1.
`line con 0`	A heading for any configuration settings for the console port. There are no console port settings.

`line vty 0 32`
 	
`!`
`end`
	A heading for any configuration settings for VTY sessions. There are no VTY session settings.

Changing a management interface IP address on the NET MGMT port

Some devices include an eth0 (NET MGMT) management interface port. This section describes how to set an IP address on that port. If your device does not have a NET MGMT management interface port, you can manage it via VLAN1 (see "How to change a management interface IP address on VLAN1" on page 22).

1. **If desired, check the current configuration.**

After logging in, enter Privileged Exec mode by using the command:

```
awplus> enable
```

Then check the current configuration by using the command:

```
awplus# show ip interface eth0 brief
```

If an address is already set, this results in the following output:

```
Interface              IP-Address      Status          Protocol
eth0                   172.28.8.200    admin up        running
```

2. **Enter Interface Configuration mode for the eth0 interface.**

Enter Global Configuration mode and enter the command:

```
awplus(config)# interface eth0
```

3. **Enter the IP address and mask.**

Enter the command:

```
awplus(config-if)# ip address <address/mask>
```

For example, to set the address to 172.28.8.210/12, enter the command:

```
awplus(config-if)# ip address 172.28.8.210/12
```

How to change a management interface IP address on VLAN1

This section describes how to change an IP address on the default VLAN (vlan1) management interface.

1. **If desired, check the current configuration.**

After logging in, enter Privileged Exec mode by using the command:

```
awplus> enable
```

Then check the current configuration by using the command:

```
awplus# show ip interface vlan1 brief
```

The output looks similar to this (note that this example already has an address assigned):

```
Interface              IP-Address      Status          Protocol
vlan1                  172.28.8.200    admin up        running
```

2. **Enter Interface Configuration mode for the vlan1 interface.**

Enter Global Configuration mode and enter the command:

```
awplus(config)# interface vlan1
```

3. **Enter the IP address and mask.**

Enter the command:

```
awplus(config-if)# ip address <address/mask>
```

For example, to change the address to 172.28.8.210/12, enter the command:

```
awplus(config-if)# ip address 172.28.8.210/12
```

How to save and boot from the current configuration

This section tells you how to save your configuration and run the saved configuration when the device starts up.

You can either:

- save the configuration to the device's default configuration file (called "default.cfg"). By default, the device uses that file at start-up.
- create a new configuration file and set the device to use the new configuration file at start-up.

How to save to the default configuration file

Enter Privileged Exec mode and enter the command:

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

The parameter **startup-config** is a short-cut for the current boot configuration file, which will be the default configuration file unless you have changed it, as described in the next section.

How to create and use a new configuration file

1. **Copy the current configuration to a new file**

Enter Privileged Exec mode and enter the command:

```
awplus# copy running-config <destination-url>
```

Note: You can save the file onto flash memory, or an SD card, or USB device. The default is flash. For details about file names and paths, see the Configuration and File Management Feature Overview and Configuration Guide.

Example To save the current configuration in a file called "example.cfg", enter the command:

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

2. **Set the device to use the new file at startup**

To run the new file's configuration when the device starts up, enter Global Configuration mode and enter the command:

```
awplus(config)# boot config-file <filepath-filename>
```

Note that you can set the device to use a configuration file on an SD card or USB device if you have saved the configuration file to that card or device. You can only specify that the configuration file is on an SD card or USB device if there is a backup configuration file already specified in flash.

To set a backup configuration file to load if the main configuration file cannot be loaded, enter the command:

```
awplus(config)# boot config-file backup <filepath-filename>
```

Example To run the commands in “example.cfg” on startup, enter the command:

```
awplus(config)# boot config-file flash:/example.cfg
```

To set “backup.cfg” as the backup to the main configuration file, enter the command:

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

1. **Display the new settings**

To see the files that the device uses at startup, enter Privileged Exec mode and enter the command:

```
awplus# show boot
```

This results in the following output:

```
Boot configuration
-----------------------------------------------------------------
Current software   : x510-5.4.4-3.5.rel
Current boot image : flash:/x510-5.4.4-3.5.rel
Backup  boot image : flash:/x510-5.4.4-3.4.rel
Default boot config: flash:/default.cfg
Current boot config: usb:/example.cfg (file exists)
Backup  boot config: flash:/backup.cfg (file exists)
```

2. **Continue updating the file when you change the configuration**

When you next want to save the current configuration, enter Privileged Exec mode and enter the command:

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

The parameter **startup-config** is a short-cut for the current boot configuration file.

How to undo settings

There are two possibilities for undoing settings: the **no** parameter and the **default** parameter.

How to use the ***no*** parameter

To undo most settings, simply re-enter the first parameters of the configuration command with the parameter **no** before them.

Example You can set the timezone to Eastern Standard Time by entering the command:

```
awplus(config)# clock timezone EST minus 5
```

To remove the timezone setting, enter the command:

```
awplus(config)# no clock timezone
```

How to use the ***default*** parameter

Some commands have a **default** parameter that returns the feature to its default setting.

Example You can change the login banner to “this is a new banner” by entering the command:

```
awplus(config)# banner motd this is a new banner
```

To return to the default banner, enter the command:

```
awplus(config)# banner motd default
```

Note that this command also has a **no** parameter that lets you remove the banner altogether.

How to set passwords and create user accounts

How to change the password for the manager account

To change the password for the manager account, enter Global Configuration mode and use the following command:

```
awplus(config)# username manager password <new-password>
```

The password can be up to 31 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.

How to set strong passwords

The password security rules are disabled by default. To set password security rules for users with administrative rights, or privilege level 15, enter Global Configuration mode.

You can then either specify whether the user is forced to change an expired password at the next login, or specify whether the user is not allowed to login with an expired password. You will need to specify a password lifetime greater than 0 before selecting either of these features. Note that the **security-password forced-change** and the **security-password reject-expired-pwd** commands cannot be enabled concurrently.

Password lifetime

Enter the following command to specify the password lifetime in days:

```
awplus(config)# security-password lifetime <0-1000>
```

Note that the value 0 will disable lifetime functionality and passwords will never expire. If lifetime functionality is disabled, the **security-password forced-change** command and the **security-password warning** command are also disabled.

Password forced change

To specify that a user is forced to change an expired password at the next login, enter the following command:

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

If the **security-password forced-change** command is enabled, users with expired passwords are forced to change to a password that must comply with the current password security rules at the next login.

Reject expired password

To specify that a user is not allowed to login with an expired password, enter the following command:

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

If the **security-password reject-expired-pwd** command is enabled, users with expired passwords are rejected at login. Users then have to contact the Network Administrator to change their password.

Caution

You cannot login to the device once all users' passwords are expired and 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.

Use other password security rules to further configure password security settings.

Password warning

AlliedWare Plus can warn users that passwords will expire in a specified number of days. To specify the number of days, enter the command:

```
awplus(config)# security-password warning <0-1000>
```

The value 0 will disable warning functionality. The warning period must be less than, or equal to, the password lifetime.

Password history

To specify the number of previous passwords that are unable to be reused, enter the command:

```
awplus(config)# security-password history <0-15>
```

A new password is invalid if it matches a password retained in the password history. The value 0 will disable history functionality. If history functionality is disabled, all users' password history is reset and all password history is lost.

Password minimum length

To specify the minimum allowable password length, enter the command:

```
awplus(config)# security-password minimum-length <1-23>
```

Password minimum categories

To specify the minimum number of categories that the password must contain in order to be considered valid, enter the command:

```
awplus(config)# security-password minimum-categories <1-4>
```

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.

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.

How to add a user is described in "How to add and remove users" on page 29.

Display security password settings

To list the configuration settings for the various security password rules, enter the command:

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

To list users' remaining lifetime or last password change, enter the command:

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

How to add and remove users

Adding users

To add a new user with administrative rights, enter Global Configuration mode and enter the command:

```
awplus(config)# username <name> privilege 15 password <password>
```

Both <***name***> and <***password***> can contain any printable character and are case sensitive.

When you add a user with administrative rights, <***password***> will have to conform to the following rules:

- **security-password minimum-categories** command
- **security-password minimum-length** command
- **security-password history** command. If this command is enabled, <***password***> is invalid if it matches a password retained in the password history.

The AlliedWare Plus OS gives you a choice of privilege levels of 1-15. Level 1-6 users are limited to User Exec mode and can only access some show commands. Level 7-14 users can access a majority of show commands. Level 15 users have access to all show and configuration commands.

Note that some show commands, such as **show running-configuration** and **show startup-configuration**, are only available at privilege level 15.

For example, to add user Bob with password 123$%^, enter the command:

```
awplus(config)# username Bob privilege 15 password 123$%^
```

Removing users

To remove a user, enter Global Configuration mode and enter the command:

```
awplus(config)# no username <name>
```

For example, to remove user Bob, enter the command:

```
awplus(config)# no username Bob
```

Note that you can delete all users, including the user called 'manager' and the user you are logged in as. If all privilege 15 user accounts are deleted, a warning message is generated:

```
% Warning: No privileged users exist.
```

If all privilege level 15 user accounts are deleted, and there are no other users configured for the device, you may have to reboot with the default configuration file.

You can also set a password for the step of moving from User Exec mode to Privileged Exec mode. This enables users with privilege level 1-6 to access Privileged Exec mode by entering the password.

To set the password, use the commands:

```
awplus# configure terminal
awplus(config)# enable password <password>
```

When low-privilege-level users log in, they can access the Privileged Exec mode by entering the **enable** command with the password. For example, if the password is 'mypassword', they would enter:

```
awplus> enable mypassword
awplus#
```

Displaying users

To list the currently logged-in users, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show users
```

The output looks like this:

```
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
```

To list all configured users, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show running-config|include username
```

The output looks like this:

```
username manager privilege 15 password 8 $1$bJoVec4D$JwOJGPr7YqoExA0GVasdE0
username Bob privilege 15 password 8 $1$gXJLY8dw$iqkMXLgQxbzSOutNUa5E2.
```

Pre-encrypted passwords

The running-config output above includes the number 8 after the **password** parameter. This indicates that the password is displayed in its encrypted form.

You can enter the number 8 and a pre-encrypted password on the command line. You may want to pre-encrypt passwords if you need to load them onto devices via an insecure method (such as HTTP, or by emailing them to remote users).

Caution

Only enter the number 8 if you are entering a pre-encrypted password—otherwise, you will be unable to log in using the password and will be unable to access the device through that username. The next section describes why.

Testing this feature

If you want to test the effect of this, **create a new user** for the test instead of using the manager user (or another existing user). The test stops you from logging in as the test user, so you need to have the manager user available to log in as.

The following output shows how specifying the number 8 puts the password into the running-config exactly as you typed it:

```
awplus(config)#username Bob privilege 15 password 8 friend
awplus(config)#show running-config |include username Bob
username Bob privilege 15 password 8 friend
```

After entering the command above, logging in as ‘Bob’ with a password of ‘friend’ does not work. This is because the device takes the password you enter (‘friend’), hashes it, and compares the hash with the string in the running-config (‘friend’). The hashed value and ‘friend’ are not the same, so the device rejects the login.

How to view system information

This section describes how to view the following system information:

- overview information
- details of temperature and voltage
- serial number

Viewing overall system information

To display an overview of the device hardware, software, and system settings, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show system
```

The output depends on the product, but is similar to this:

```
System Status                                    Wed Sep 28 12:44:10 2022

Board       ID  Bay   Board Name                          Rev   Serial number
-------------------------------------------------------------------------------
Chassis    315        AT-SBx8112                          E-0   A042764112500070
Blade      317  Bay1  AT-SBx81GP24                        D-0   A042774112800031
Blade      353  Bay2  AT-SBx81XS6                         X8-0  A045624113500003
Blade      317  Bay3  AT-SBx81GP24                        D-0   A042774112700005
Controller 316  Bay5  AT-SBx81CFC400                       F-0   A042854111300027
Controller 316  Bay6  AT-SBx81CFC400                       F-0   A042854111300029
Blade      352  Bay7  AT-SBx81GS24a                       C-1   A042824112400004
Blade      351  Bay11 AT-SBx81GT24                        B-1   A044024110900001
Blade      352  Bay12 AT-SBx81GS24a                       C-1   A042824104600004
PSU        319  PSU4  AT-SBxPWR-SYS/AC                    A-0   -
Fan module 321  PSU5  AT-SBxFAN12                         E-0   A042844112400016
-------------------------------------------------------------------------------
RAM:  Total: 513436 kB Free: 365932 kB
Flash: 126.0MB Used: 121.2MB Available: 4.8MB
-------------------------------------------------------------------------------
Environment Status : Normal
Uptime             : 0 days 00:03:26
Bootloader version : 2.0.23


Current software   : SBx81CFC400-5.5.2-0.1.rel
Software version   : 5.5.2
Build date         : Fri Apr 8 2022 18:12:19 NZST

Current boot config: flash:/default.cfg (file exists)

System Name
 awplus
System Contact

System Location
```

Viewing voltage, fan status, power supply, alarm status, and temperature

The device monitors the environmental status of its power supplies and fan.

To display this information, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show system environment
```

The output depends on the product, but is similar to this:

```
awplus#show system environment
Stack Environment Monitoring Status

Stack member 1:

Overall Status: Normal
System Airflow: Front to back

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
```

Viewing the serial number

The device's serial number is displayed in the output of the **show system** command, but for convenience, you can also display it by itself.

To do this, enter User Exec or Privileged Exec mode and enter the command:

```
awplus# show system serialnumber
```

The output looks like this:

```
P1FY7502C
```

How to set system parameters

You can set system parameters to personalize the device and make it easy to identify it when troubleshooting.

This section describes how to configure the following system parameters:

- Telnet session timeout
- Device name
- Login banner

How to change the Telnet session timeout

By default, Telnet sessions time out after 10 minutes of idle time. If desired, you can change this.

To change the timeout for all Telnet sessions, enter Global Configuration mode and enter the commands:

```
awplus(config)# line vty 0 32
awplus(config-line)# exec-timeout <new-timeout>
```

The new timeout value only applies to new sessions, not current sessions.

Examples To set the timeout to 30 minutes, enter the command:

```
awplus(config-line)# exec-timeout 30
```

To set the timeout to 30 seconds, enter the command:

```
awplus(config-line)# exec-timeout 0 30
```

To set the timeout to infinity, so that sessions never time out, enter either of the commands:

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

How to name the device

To give the device a name, enter Global Configuration mode and enter the command:

```
awplus(config)# hostname <name>
```

For example, to name the device “mycompany”

```
awplus(config)# hostname mycompany
```

The prompt displays the new name:

```
my company(config)#
```

The name can contain hyphens and underscore characters, for example:

```
mycompany(config)#hostname mycompany_more_words
mycompany_more_words(config)#hostname mycompany-hyphenated
mycompany-hyphenated(config)
```

However, the name must be a single word (i.e. no spaces), as the following example shows:

```
mycompany(config)#hostname mycompany more words
                                   ^
% Invalid input detected at '^' marker.
```

It also cannot be surrounded by quote marks, as the following example shows:

```
awplus(config)#hostname "mycompany more words"
% hostname contains invalid characters
```

Removing the name

To remove the hostname, enter the command:

```
my company(config)# no hostname
```

The prompt changes back to the default prompt:

```
awplus(config)#
```

How to display a text banner at login

By default, the device displays the AlliedWare Plus OS version and build date before login. You can customize this by changing the Message of the Day (MOTD) banner. To enter a new MOTD banner, enter Global Configuration mode and enter the command:

```
awplus(config)# banner motd <banner-text>
```

The text can contain spaces and other printable characters. You do not have to surround words with quote marks.

Example To display “this is a new banner” when someone logs in, enter the command:

```
awplus(config)# banner motd this is a new banner
```

This results in the following output at login:

```
awplus login: manager
Password:
this is a new banner
awplus>
```

Removing the banner

To return to the default banner (AlliedWare Plus OS version and build date), enter the command:

```
awplus(config)# banner motd default
```

To remove the banner instead of replacing it, enter the command:

```
awplus(config)# no banner motd
```

How to set the time and date

There are three aspects to setting the time and date:

- setting the current time and date
- setting the timezone
- configuring the device to automatically change the time when summer-time begins and ends

Instead of manually setting the time, you can use NTP to automatically get it from another device.

How to show current settings

To display the current time, timezone and date, enter Privileged Exec mode and enter the command:

```
awplus# show clock
```

The output looks like this:

```
UTC Time:   Wed,  16 May 2022 16:08:14 +0000
Timezone: UTC
Timezone Offset: +00:00
Summer time zone: None
```

How to set the time and date

Note that IE200 and IE300 Series switches do not retain time settings over a cold reboot. We recommend using NTP on these products.

To set the time and date, enter Privileged Exec mode and enter the **clock set** command:

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

where:

- ***hh*** is two digits giving the hours in 24-hour format (e.g. **14**)
- ***mm*** is two digits giving the minutes
- ***ss*** is two digits giving the seconds
- ***day*** is two digits giving the day of the month
- ***month*** is the first three letters of the month name (e.g. **sep**)
- ***year*** is four digits giving the year

Example To set the time to 14:00:00 on 25 January 2025, use the command:

```
awplus# clock set 14:00:00 25 jan 2025
```

How to set the timezone

To set the timezone, enter Global Configuration mode and enter the **clock timezone** command:

```
clock timezone <timezone-name> {plus|minus} <0-12>
```

- The <***timezone-name***> can be any string up to 6 characters long.
- To return the timezone to UTC+0, enter the command:

```
awplus(config)# no clock timezone
```

Example To set the timezone to Eastern Standard Time, use the command:

```
awplus(config)# clock timezone EST minus 5
```

How to configure summer-time

There are two approaches for setting summer-time:

- **recurring**, when you specify the week when summer-time starts and ends and each year the device changes the time at those weeks. For example, Eastern Daylight Time (EDT) starts at 2 am on the second Sunday in March and ends at 2 am on the first Sunday in November.
- **date-based**, when you specify the start and end dates for summer-time for a particular year. For example, Eastern Daylight Time (EDT) starts at 2 am on 13 March 2022 and ends at 2 am on 6 November 2022.

Recurring To set summer-time with recurring dates, enter Global Configuration mode and enter the **clock summer-time recurring** command:

```
clock summer-time <zone-name> recurring <start-week> <start-day> <start-
month> <start-time> <end-week> <end-day> <end-month> <end-time> <1-180>
```

- The ***<zone-name>*** can be any string up to 6 characters long.
- The ***<start-time>*** and ***<end-time>*** are in the form hh:mm, in 24-hour time.

Note that if you specify 5 for the week, this changes the time on the last day of the month, not the 5th week.

Example To configure EDT, enter the command:

```
awplus(config)# clock summer-time EDT recurring 2 Sun Mar 02:00 1 Sun Nov
02:00 60
```

Date-based To set summer-time for a single year, enter Global Configuration mode and enter the **clock summer-time date** command:

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

- The <***zone-name***> can be any string up to 6 characters long.
- The <***start-time***> and ***<end-time>*** are in the form hh:mm, in 24-hour time.

Example For example, to configure EDT for 2022 enter the command:

```
awplus(config)# clock summer-time EDT date 13 Mar 2022 02:00 6 Nov 2022 02:00 60
```

How to install your device securely

This section describes how to:

- physically and logically secure your device
- secure services from the factory default state
- disable services that are enabled by default

Physical and logical security

The device is designed to function in a physically secure location to prevent the risk of outside interference with device power, cabling or ports. Certain protocols (e.g. AMF Plus, AWC) also rely on logical separation (e.g. VLANs, routing, ACLs) of the control network from general traffic. Care should be taken to differentiate AMF-internal and publicly accessible ports.

The GUI uses HTTP-based transport protocols. For best security, it is recommended that access is restricted to local devices on a trusted network (by using ACLs for example), and that the service is configured to restrict access to HTTPS only. Use the following commands to disable HTTP:

```
awplus# configure terminal
awplus(config)# http port none
```

Bootloader security relies on physical access to the device console port. Bootloader updates should only be done under direct instruction of AT support staff.

Securing services from the factory default state

The section “The default configuration” outlines the default configuration applied to a device in ‘factory default’ state. It is recommended that you disable all services and network interfaces that are not required in your deployment, to improve security and performance.

To disable ports that are not needed:

```
awplus# configure terminal
awplus(config)# interface port1.0.8
awplus(config-if)# shutdown
```

On wireless routers, the Wi-Fi radios can also be disabled:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap 100
awplus(config-wireless-ap)# radio 2
awplus(config-wireless-ap-radio)# force-disable
```

Disabling services that are enabled by default

Services that are enabled by default can be disabled. The following sections give the commands to disable these services.

Telnet Telnet allows remote terminal configuration, but it is considered insecure. It is disabled by default.

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

SSH SSH allows remote terminal and NETCONF configuration.

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

To restrict ssh to using modern secure ciphers, use:

```
awplus(config)# nssh server secure-algs
```

HTTP/ HTTPS The HTTP/HTTPS service allows GUI and RESTCONF configuration.

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

To restrict HTTP/TLS to using modern, secure ciphers, use:

```
awplus(config)# http tls-version-minimum 1.3
```

AOC Allied One Connect - Onboarding (AOC) allows remote provisioning via SZTP. It is automatically disabled once the device leaves factory-default state, by saving any configuration.

AMF Plus The AMF Plus client allows integration with existing AMF and AMF Plus networks.

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

AWC Wireless controller The AWC client allows integration with existing AWC networks.

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# management remote-sessions 0
```

This will result in AWC rejecting all non-local connections. It is also possible to reject AWC traffic at the network level using a firewall. Refer to the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide and deny inbound and outbound traffic on ports 9473, 65437, 65438, 65439 and 65440.

ISAKMP ISAKMP is an internal part of the VPN functionality. It is possible to reject traffic to the ISAKMP port at the network level using a firewall. Refer to the Firewall and Network Address Translation (NAT) Feature Overview and Configuration Guide and deny inbound and outbound traffic on port 500.

SNMP The SNMP service allows remote monitoring and management of the device via the SNMP protocol. If enabled, SNMP should be configured to use SNMPv3 with a shared secret of sufficient complexity to mitigate brute-force attacks (e.g. at least 16 characters and multiple character types).

```
awplus# configure terminal
awplus(config)# no snmp-server
```

Console The console port is always enabled and should be protected by controlling physical access.

How to enable Secure Mode

Caution 

On x930 Series switches, before enabling Secure Mode, make sure that your switch is running bootloader version 3.1.3 or later. You can see the bootloader version by running the command **show system**. If your bootloader version is earlier than 3.1.3, please contact Allied Telesis technical support for assistance.

You can put a number of AlliedWare Plus devices into Secure Mode, to make the device as secure as possible by using the strongest encryption algorithms available. Weak hashing functions such as MD5 and broken cryptographic algorithms such as RC2, DES, DSA, etc, are no longer considered secure, as they can be susceptible to brute force attacks and collisions. Secure Mode only allows you to use hashes from the SHA-2 family, and AES block cipher algorithms instead of the weaker DES cryptographic algorithms.

Block cipher algorithms encrypt data on a per-block basis. Blocks, which are measured in bits, determine the input of plain text and output of cipher text. So, for example, if you used AES128, then for every 128 bits of plain text, 128 bits of cipher text are produced.

Secure Mode meets the Common Criteria standard. Common Criteria is an internationally recognized set of guidelines for the security of information technology products.

What Secure Mode disables

When in Secure Mode, the following are disabled:

- Telnet
- SSHv1
- SNMPv1/v2
- All privilege levels except 1 and 15
- Algorithms that are not supported under FIPS, including MD5, RSA-1 and DSA
- The ability to store passwords in cleartext and to specify an **enable** password

In Secure Mode, the web server on the device (used by the Device GUI) only accepts AES128-SHA ciphers.

Note: Stacking is not supported in Secure Mode.

Entering Secure Mode

1. **On x930 Series switches, must be running bootloader version 3.1.3 or later.**

   You can see the bootloader version by running the command show system.

   Do not enable Secure Mode if your device has an older bootloader. Instead, contact Allied Telesis technical support for assistance.

2. **Obtain the correct release file and its sha256sum file by downloading them from the**

   Allied Telesis Support Portal.

   Save the files on a trusted USB device and connect the USB device to the device.

3. **Erase the device's flash.**

   To do this, boot the device into the bootloader diagnostics menu, using Ctrl-D. Select option 7 'Bootup stage 2 diagnostics menu', and then select option 4 'Erase FLASH (Filesystem only)'.

4. **Then select option 0 'Restart' to reboot the device.**

   Enter the main bootloader menu by using Ctrl-B. Select option 1 'Perform one-off boot from alternate source' and then select the 'USB' option and the release you saved in step 1.

5. **Once the device has booted up, save the release file to flash and verify it, as described in** "How to verify the firmware file" on page 43**.**

6. **Set the verified release as the boot release.** For example, use the following commands:

```
awplus#configure terminal
awplus(config)#boot system x550-5.4.8-1.2.rel
```

7. **Use the following commands to enter Secure Mode:**

```
awplus(config)# crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

8. **Use the following command to confirm that the device is in Secure Mode:**

```
awplus# show secure-mode
```

   The following message should be displayed: `Secure mode is enabled`

Leaving Secure Mode

1. **If you wish to leave Secure Mode, you should delete all sensitive information first.**

   This means deleting all trustpoints (one by one), by using the commands:

```
awplus# configure terminal
awplus(config)# no crypto pki trustpoint <name>
```

   Also, delete all public/private key pairs, by using the commands:

```
awplus# crypto key zeroize all
```

2. **Turn off Secure Mode, by using the commands:**

```
awplus(config)# no crypto secure-mode
awplus(config)# exit
awplus# write
awplus# reboot
```

3. **Reboot the device.**

   The device ***must*** be rebooted after Secure Mode is turned off, and ideally flash memory should be erased via the bootloader, as described above.

How to verify the firmware file

You can verify the firmware file to ensure that it has not been corrupted or interfered with during download. To do this, enter Global Configuration mode and enter the following command to verify the SHA256 checksum of the file:

```
awplus(config)# crypto verify <filename> <hash-value>
```

where <***hash-value***> is the known correct checksum of the file.

This command compares the SHA256 checksum of the firmware file with the correct checksum for the file.

The correct checksum is listed in the firmware's sha256sum file, which is available from the Allied Telesis Support Portal. It is also in the firmware version's release note.

Caution If the verification fails, the following error message will be generated:

"% Verification Failed".
If this happens, please delete the release file and contact Allied Telesis support

All device models of a particular series run the same firmware file and therefore have the same checksum. For example, all x930 Series switches have the same checksum.

To validate a downloaded GUI resource file use:

```
awplus(config)# crypto verify <filename> <hash-value>
```

The correct checksum is listed in the release note for that GUI release, which is available from the Allied Telesis Support Portal.

Verifying the firmware on subsequent bootups

Once the device has successfully verified the firmware file, it adds the **crypto verify** command to the running configuration. To verify the firmware file on every bootup, save the configuration file as the startup configuration, using the command:

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

If the **crypto verify** command is in the startup configuration and verification of the boot release fails on startup, the device will reboot. Contact Allied Telesis support if this happens.

Verifying the GUI on subsequent bootups

To verify the active GUI resource file use:

```
awplus(config)# crypto verify gui <hash-value>
```

To verify the GUI file on every bootup, save the configuration file as the startup configuration, using the command:

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

If the **crypto verify gui** command is in the startup configuration and verification of the GUI file fails on startup, the device will disable the HTTP service. To recover from this situation, either:

- If a new GUI file has been downloaded, update the startup configuration file with the new hash
- Otherwise download the GUI file again, replace the corrupted file and verify it again.

Once you have a verified GUI file, re-enable the HTTP service using:

```
awplus(config)# service http
```

How to work with files

The AlliedWare Plus OS lets you create directory trees for file storage. This section summarizes file operations; for more detailed information, see the Configuration and File Management Feature Overview and Configuration Guide.

This section describes:

How to list files

Listing files

To list files, enter Privileged Exec mode and enter the command:

```
awplus# dir
```

The output lists files and directories in order of modification date, descending. It looks like this:

```
-rw- 534 Jul 12 2022 17:52:50 stp.cfg
-rw- 534 Jul 12 2022 17:12:50 example.cfg
-rw- 12429011 Jul 12 2022 16:26:06 r1-5.2.1-rc3.rel
```

Displaying information about the file system

To display information about the different memory types on the device, enter Privileged Exec mode and enter the command:

```
awplus# show file systems
```

The output includes the amount of free memory and the prefix you type to access that memory type, and looks like this:

```
awplus#show file systems
 Size(b)   Free(b)   Type    Flags  Prefixes    S/D/V    Lcl/Ntwk  Avail
-----------------------------------------------------------------------
  63.0M     28.5M   flash     rw  flash:      static  local      Y
      -         -   system    rw  system:     virtual local      -
  10.0M      9.8M   debug     rw  debug:      static  local      Y
 499.0K    431.0K   nvs       rw  nvs:        static  local      Y
      -         -   tftp      rw  tftp:       -       network    -
      -         -   scp       rw  scp:        -       network    -
      -         -   sftp      ro  sftp:       -       network    -
      -         -   http      ro  http:       -       network    -
      -         -   rsync     rw  rsync:      -       network    -
```

Listing files in a subdirectory

To list the contents of a directory, enter Privileged Exec mode and enter the command:

```
awplus# dir <directory-name>
```

Note: You can specify the directory with or without a / after the directory name.

Example To display the contents of a directory called ‘example’, enter the command:

```
awplus# dir example
```

Listing files in NVS memory or on an SD card

To list the contents of a directory in NVS (non-volatile storage), enter Privileged Exec mode and enter the command:

```
awplus# dir nvs:<directory-name>
```

To list the contents of a directory on an SD card, enter the command:

```
awplus# dir card:<directory-name>
```

Example To display the contents of a directory in NVS called “example”, enter the command:

```
awplus# dir nvs:example
```

How to display the contents of configuration and text files

To display the contents of a file, enter Privileged Exec mode and enter the command:

```
awplus# show file <filename>
```

Example To display the contents of the file called “example.cfg”, enter the command:

```
awplus# show file example.cfg
```

How to navigate through the file system

Showing the current directory

To see which directory you are currently in, enter Privileged Exec mode and enter the command:

```
awplus# pwd
```

For the top-level directory, the output looks like this:

```
flash:
```

Changing directories

To change to another directory, enter Privileged Exec mode and enter the command:

```
awplus# cd <directory-name>
```

To go to a directory one level higher in the directory tree, enter the command:

```
awplus# cd ..
```

Example To change to a directory called ‘example’, enter the command:

```
awplus# cd example
```

To go up one level, which returns you to the top level directory, enter the command:

```
awplus# cd ..
```

Changing to a directory in NVS memory or on an SD card

To change to the top-level directory in the NVS memory file system, enter Privileged Exec mode and enter the command:

```
awplus# cd nvs:
```

To change to the top-level directory on an SD card, enter the command:

```
awplus# cd card:
```

Note that the prefix for the SD card is “card” not “sdcard”. Next, you can change to other directories in NVS memory or on the SD card, by entering the command:

```
awplus# cd <directory-name>
```

Alternatively, you can go straight from flash to a subdirectory in the alternative file system, by entering one of the commands:

```
awplus# cd nvs:<directory-name>
awplus# cd card:<directory-name>
```

To return to the flash file system, enter the command:

```
awplus# cd flash:
```

Example To change to the directory within NVS called ‘example’, enter the command:

```
awplus# cd nvs:example
```

To go up one level, which returns you to the top-level directory of NVS memory, enter the command:

```
awplus# cd ..
```

Creating new directories

To create a directory, enter Privileged Exec mode and enter the command:

```
awplus# mkdir <directory-name>
```

Example To make a directory called “example” within the flash file system, enter the command:

```
awplus# mkdir example
```

Deleting directories

To delete an empty directory, enter Privileged Exec mode and enter the command:

```
awplus# rmdir <directory-name>
```

To delete a directory and all its contents, enter Privileged Exec mode and enter the command:

```
awplus# delete recursive <directory-name>
```

The device prompts you for confirmation.

Example To delete an empty directory called ‘example’ from within the flash file system, enter the command:

```
awplus# rmdir example
```

How to copy files

Within a directory To copy a file within the same directory, enter Privileged Exec mode and enter the command:

```
awplus# copy <source-filename> <destination-filename>
```

If the file already exists, the device asks whether to overwrite it, with a message like this:

```
Overwrite flash:/example.cfg? (y/n)[n]:
```

To overwrite, press the ‘y’ key then the Enter key.

Between directories To copy a file to another directory within the same file system, enter the command:

```
awplus# copy <source-filename> <directory-name>/
```

The / after the directory name is required. Otherwise the device displays an error:
`("37: Destination file is a directory").`

The device then prompts you for the destination filename. To give the copy a new name, type the name at the prompt. You can include directory names in the path.

To use the same filename as the original, press the Enter key (do not press the ‘y’ key—that names the copy ‘y’).

Example To put a copy of example.cfg into the example directory, enter the command:

```
awplus# copy example.cfg example/
```

The prompt and messages look like this:

```
Enter destination file name [example.cfg]:
Copying from source file, please wait...
Copying to destination file, please wait...
0: Successful operation
```

Copying to and from NVS, SD card or USB memory device

To copy between file systems, you need to specify the file system prefix (nvs: or card: or usb:).

For example, to copy from flash to NVS when your current directory is the top-level flash directory, enter Privileged Exec mode and enter the command:

```
awplus# copy <source-filename> nvs:
```

The device prompts you for the filename, as described in the previous section.

To copy from NVS to flash when your current directory is the top-level flash directory, enter the command:

```
awplus# copy nvs:<source-filename> <destination-filename>
```

Example To copy the file 'example.txt' from the directory in NVS called 'example' to the top level of flash, enter the command:

```
awplus# copy nvs:example/example.txt example.txt
```

Copying to and from a TFTP server

To copy a file from a TFTP server to flash memory, enter Privileged Exec mode and enter the command:

```
awplus# copy tftp flash
```

The device prompts you for the:

- TFTP server hostname (you can enter its IP address instead)
- source filename on the TFTP server
- destination filename in flash on the device

To copy a file from flash to a TFTP server, enter the command:

```
awplus# copy flash tftp
```

Follow the prompts for source filename, server, and destination filename.

Note: You can specify the server and filename in the command instead of waiting for prompts. Use a format like the following:

```
copy tftp://172.1.1.1/example.cfg flash
```

Example To copy example.cfg to the TFTP server at 172.1.1.1, enter the command:

```
awplus# copy flash tftp
```

The prompts, responses, and messages look like this:

```
Enter source file name []:example.cfg
Enter destination host name []:172.1.1.1
Enter destination file name [example.cfg]:
Copying from source file, please wait...
Copying to destination file, please wait...
0: Successful operation
```

How to use the editor

The inbuilt editor is JOE (Joe's Own Editor).

To edit an existing file, enter Privileged Exec mode and enter the command:

```
awplus# edit <filename>
```

To open the editor with a empty file, enter the command:

```
awplus# edit
```

When you save the new file, you may need to specify the file system to store it on. For flash, use **flash:*<filename>***.

Using JOE Use control-character sequences to format and manipulate text in JOE. The following table summarizes a few useful sequences—for details, see:

https://joe-editor.sourceforge.io/4.6/man.html

FUNCTION	CONTROL-CHARACTER SEQUENCE
Access the Help	Ctrl-K-H
Saving the file without exiting (for new files, this prompts for a filename).	Ctrl-K-D
Save the file and exit (this prompts for a filename)	Ctrl-K-X
Exit without saving the file	Ctrl-C
Go to the beginning of the file	Ctrl-K-U
Go to the end of the file	Ctrl-K-V
Go up one screenful of text in the file	Ctrl-U
Go down one screenful of text in the file	Ctrl-V
Select a block of text:	
Mark the beginning of the block	Ctrl-K-B
- Mark the end of the block	Ctrl-K-K
- Copy and paste a selected block of text	Place cursor at destination then enter: Ctrl-K-C
Move a selected block of text	Place cursor at destination then enter: Ctrl-K-M
Delete a selected block of text	Ctrl-K-Y

How to enable the USB port of TQR Series access points

From version 5.5.5-2.1 onwards, the USB port is disabled by default on TQR Series devices, to enhance security. To enable the port, use the following commands:

```
awplus# configure terminal
awplus(config)# wireless
awplus(config-wireless)# ap-profile local
awplus(config-wireless-ap-prof)# usb-port enable
```

How to return to the factory defaults

Completely restore defaults

To return to factory settings, enter Privileged Executive mode and use the command:

```
awplus# erase factory-default
```

This command erases all data from NVS and all data from flash excluding the following:

- The current release file
- The backup release file
- license

The device is then rebooted and returned to its factory default condition as follows:

```
awplus login: manager
Password:
Last login: Thu Jul  6 00:54:10 UTC 2017 on ttyS0

AlliedWare Plus (TM) 5.4.7 06/09/17 05:35:30

awplus>en
awplus#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.
Proceed ? (y/n):y
.
.
.
Loading default configuration
Warning: flash:/default.cfg does not exist, loading factory defaults.
..

done!
Received event network.configured
```

Note: After reboot, the **show running-config** output will display the default factory settings for your device once you have removed the default.cfg file. To recreate the default.cfg file enter **copy running-config startup-config**. When you enter copy running-config, startup-config, commands the default.cfg file is updated with the startup-config.

Restore default configuration

The device dynamically adds the default settings to the running-config at start-up if the default file is not present. You can use this feature to completely remove your configuration and return to the factory default configuration, without removing any other files. To do this, delete or rename the default file and make sure no other file is set as the start-up configuration file.

- Find the location of the default boot configuration file, by entering Privileged Exec mode and entering the command:

```
awplus# show boot
```

- Delete the default file when it is the current boot configuration file, by entering Privileged Exec mode and entering either of the commands:

```
awplus# delete force <filename>
```

or

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

Caution Erasing startup-config **deletes** the current boot configuration file—it does not simply stop the file from being the boot file.

To make sure that no other file is loaded at start-up, enter Global Configuration mode and enter the command:

```
awplus(config)# no boot config-file
```

Partially restore defaults

To partially restore the default settings, make a configuration file that contains the settings you want to keep and set this as the start-up configuration file. On start-up, the device will add the missing settings to the running-config.

For example, to use default settings but still keep an IP address on the eth0 (NET MGMT) management port, create a file like the following one and set it as the boot configuration file:

```
!
interface eth0
 ip address 172.28.8.210/16
!
ip route 0.0.0.0/0 172.28.0.1
!
end
```

How to upgrade the firmware

New releases of the AlliedWare Plus OS become available regularly.

On AR4050S and TQR series devices, the AlliedWare Plus Update Manager will periodically check for newer firmware releases. If a newer firmware release is available you will see a notification via an alert log message which will appear on the CLI. The GUI will also display a banner message. To upgrade, download the firmware file and install it manually using the following steps.

1. **Put the new release onto your TFTP server or your USB drive.**

2. **If necessary, create space in the device's flash memory for the new release.**

Note that you cannot delete the current release file. To see how much space is free, use the command:

```
awplus# show file systems
```

3. **Copy the new release from your TFTP server or your USB drive onto the device.**

To copy the release file from a TFTP server to flash memory, enter Privileged Exec mode and enter the command:

```
awplus# copy tftp flash
```

To copy the release file from a USB device, when your current directory is the top-level flash directory, enter the command:

```
awplus# copy usb:<source-filename> flash
```

On SBx8100 Series switches, you only need to copy the new release to the Active SBx81CFC960 Control Fabric Card (CFC). If your SBx8100 system has a standby CFC installed, the new release file, the configuration file, and all licenses are automatically synchronized from the Active CFC.

4. **Set the device to boot from the new release.**

Enter Global Configuration mode and enter the command:

```
awplus(config)# boot system <filepath-filename>
```

Note: If the device is in Secure Mode, the file will first have to be verified. See "How to verify the firmware file" on page 43

5. **Check the boot settings.**

Enter Privileged Exec mode and enter the command:

```
awplus# show boot
```

6. **Reboot.**

Enter Privileged Exec mode and enter the command:

```
awplus# reboot
```

How to easily locate the device in a server room

The **Find Me** feature enables you to physically locate a specific device from a group of similar devices.

When you use the **findme** command, the device's LEDs alternately flash green and amber at a rate of 1 Hz. If the device has no amber LED, then the green LED will flash on/off at a rate of 1 Hz.

An optional **interface** parameter specifies one or more interfaces to flash, while an optional **member** parameter specifies a particular stack member. Both these parameters are mutually exclusive. If no **interface** or **member** parameter is specified, then all ports on the device or stack are flashed.

An optional **timeout** parameter specifies the flash behavior **duration**. The default time is one minute (60 seconds). Normal LED behavior is restored automatically after either the default time, or a specified time, has elapsed or a **no findme** command is used.

How to filter and save ‘show’ command output

You can control the output of **show** commands by using the **|** and **>** or **>>** tokens in the following ways:

- To display only part of the output, follow the command with **|** and then other keywords (see: **Output modifiers** below)
- To save the output to a file, follow the command with **> filename**
- To append the output to an existing file, follow the command with **>> filename**

Using the ? after typing the **show** command displays the following information about these tokens.

```
awplus# show users
```

```
| Output modifiers
> Output redirection
>> Output redirection (append)
```

Output modifiers

Type the | (vertical bar) to use output modifiers.

```
append    Append output
begin     Begin with the first line that contains
          matching output
exclude   Exclude lines that contain matching output
include   Include lines that contain matching output
redirect  Redirect output
```

Begin The **begin** parameter causes the display to begin at the first line that contains the input string.

```
awplus# show run | begin vlan1
```

```
...skipping
interface vlan1
 ip address 192.168.14.1
!!
line con 0
 login
line vty 0 4
 login
!
end
```

Exclude

The **exclude** parameter excludes all lines of output that contain the input string. In the following output all lines containing the word “input” are excluded:

```
awplus# show interface vlan1 | exclude input
```

```
Interface vlan1
  Scope: both
  Hardware is Ethernet, address is 192.168.14.1
  index 3 metric 1 mtu 1500 <UP,BROADCAST,RUNNING,MULTICAST>
  Label switching is disabled
  No Virtual Circuit configured
  Administrative Group(s): None
  DSTE Bandwidth Constraint Mode is MAM
    output packets 4438, bytes 394940, dropped 0
    output errors 0, aborted 0, carrier 0, fifo 0, heartbeat 0, window 0
    collisions 0
```

Include

The include parameter includes only those lines of output that contain the input string. In the output below, all lines containing the word “input” are included:

```
awplus# show interface vlan1 | include input
```

```
input packets 80434552, bytes 2147483647, dropped 0, multicast packets 0
input errors 0, length 0, overrun 0, CRC 0, frame 0, fifo 1, missed 0
```

Redirect

The **redirect** parameter puts the lines of output into the specified file. If the file already exists, the new output overwrites the file’s contents; the new output is not appended to the existing file contents.

| redirect and **>** are synonyms

```
awplus# show history | redirect history.txt
```

Output redirection

The output redirection token **>** puts the lines of output into the specified file. If the file already exists, the new output overwrites the file’s contents; the new output is not appended to the existing file contents.

| redirect and **>** are synonyms

```
awplus# show history > history.txt
```

Append output

The append output token **>>** adds the lines of output into the specified file. The file must already exist, for the new output to be added to the end of the file’s contents; the new output is appended to the existing file contents.

| append and **>>** are synonyms.

```
awplus# show history >> history.txt
```