Management Software

AT-S83

Command Line Interface User's Guide

AT-10408XP 10-Gigabit Ethernet Switch

Version 1.0.0

613-000546 Rev. A

Allied Telesis™

Contents

Tables

Preface

The AT-S83 Management Software is a command line software that is designed for use with the AT-10408XP 10-Gigabit Ethernet Switch. This guide provides a description of the commands.

The preface contains the following sections:

Safety Symbols Used in this Document

This document uses the safety symbols defined in Table 1.

Table 1. Safety Symbols

Symbol	Meaning	Description
	Caution	Performing or omitting a specific action may result in equipment damage or loss of data.
	Warning	Performing or omitting a specific action may result in electrical shock.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesis products are available in portable document format (PDF) on our web site at **www.alliedtelesis.com**. You can view the documents online or download them onto a local workstation or server.

For details about the features and functions of the AT-10408XP switch, refer to the *AT-10408XP 10-Gigabit Ethernet Switch Installation Guide* (part number 613-000707) on our web site.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support as well as sales or corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base from the following web site: **www.alliedtelesis.com/support/kb.aspx**. You can use the Knowledge Base to submit questions to our technical support staff and review answers to previously asked questions.

Email and Telephone Support

For Technical Support via email or telephone, refer to the Allied Telesis web site: **www.alliedtelesis.com**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Warranty

For warranty information, refer to the Allied Telesis web site: **www.alliedtelesis.com/warranty**.

Returning Products

Products for return or repair must first be assigned a Return Materials Authorization (RMA) number. A product sent to Allied Telesis without a RMA number will be returned to the sender at the sender's expense.

To obtain an RMA number, contact the Allied Telesis Technical Support group at our web site: **www.alliedtelesis.com/support/rma**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

For Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information at our web site: **www.alliedtelesis.com**. Select your country from the list displayed on the website. Then select the appropriate menu tab.

Chapter 1

Getting Started with the Command Line Interface

This chapter describes the command modes of the AT-S83 command line interface and how to access them. This chapter includes the following sections:

Introducing the Command Modes

This chapter describes the CLI command modes and how to access the command line interface. There are 8 command modes:

- View
- Privileged Executive
- Configuration Terminal
- Router
- VLAN Configuration
- Interface Configuration
- Line
- Key Chain

In the AT-S83 software, the commands are accessed through a hierarchy of command modes. Each command mode contains a subset of commands that are available within that mode only. For an illustration of the command modes, see Figure 1 on page 17.

When you log on to the CLI interface, the default command mode that you access depends on your login id. There are two default login ids that are sent from the factory. The operator login id enables you to display the software. With this login, you access the View command mode automatically. The manager login id permits full administrator capabilities. With this login, you access the Privileged Executive mode by default.

To navigate from one command mode to another, you enter a specific command. For example, to access the Privileged Executive mode, you enter the ENABLE command from the View mode. Once you enter a new command mode, the AT-S83 prompt changes to indicate the new mode. See Table 2 on page 18 for information about the commands used to access the modes and their respective prompts.

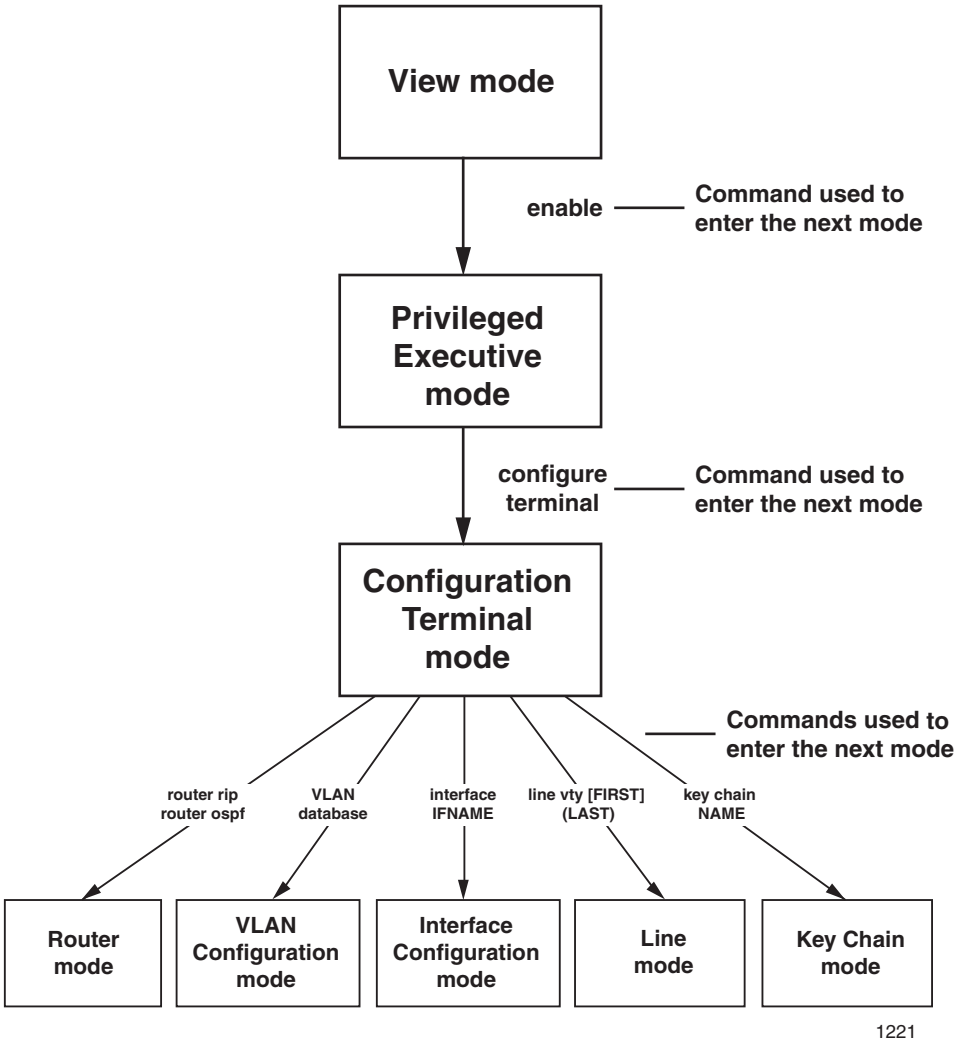

Figure 1. AT-S83 Command Modes

Table 2. Command Modes

Command Mode	Prompt	Description
View mode	Switch#	❒ This is the default command mode for the operator login. ❒ Enter the LOGOUT or EXIT commands to quit the software.
Privileged Executive mode	Switch#	❒ This is the default command mode for the manager login. ❒ Access this mode from the View mode with the ENABLE command. ❒ Enter the DISABLE or EXIT commands to return to the View mode.
Configuration Terminal Mode	Switch(config)#	❒ Use the CONFIGURE command to enter this mode from the Privileged Executive mode. ❒ To return to the Privileged Executive mode, enter the END or EXIT commands.
Router Mode	Switch(config-router)#	❒ Type the ROUTER RIP or ROUTER OSPF commands to enter this mode from the Configuration Terminal mode. ❒ To return to the Configuration Terminal mode, enter the END or EXIT commands.
Interface Configuration	Switch(config-if)#	❒ To access interface 1, enter the following from the Configuration Terminal Mode: `interface xe1` ❒ Enter the END or EXIT commands to return to the Configuration Terminal mode.
VLAN Configuration	Switch(config-vlan)#	❒ From the Configuration Terminal mode, type the VLAN DATABASE command. ❒ Enter the END or EXIT commands to return to the Configuration Terminal mode.

Table 2. Command Modes (Continued)

Command Mode	Prompt	Description
Line	Switch(config-line)	❒ From the Configuration Terminal mode, type the LINE VTY command. ❒ Enter the END or EXIT commands to return to the Configuration Terminal mode.
Key Chain	Switch(config-keychain)#	❒ To enter this mode from the Configuration Terminal mode, type the KEY CHAIN command. ❒ Enter the END or EXIT commands to return to the Configuration Terminal mode.

In addition, there are commands that allow you to move between the modes. For example, typing the EXIT command when you are in the Interface Configuration mode returns you to the Configuration Terminal mode. From the View mode, the LOGOUT command exits the software.

If you enter a command that is not accessible from a command mode, the software displays a "command not found" message. For example, you can enter the SHOW SNMP command from the Privileged Executive mode, but you cannot enter this command from the VLAN Configuration mode. Within the manual, a command mode is listed for each command.

See the following sections for a description of each command mode:

- ❒ "View Command Mode" on page 20
- ❒ "Privileged Executive Command Mode" on page 21
- ❒ "Configuration Terminal Mode" on page 22
- ❒ "Interface Configuration Command Mode" on page 22
- ❒ "Router Mode" on page 24
- ❒ "VLAN Configuration Command Mode" on page 24
- ❒ "Line Mode Commands" on page 25
- ❒ "Key Chain Mode Command" on page 26

View Command Mode

The View command mode is the default command mode for the operator login id. It permits access to basic commands. To indicate the View mode, the prompt changes to “Switch>.” All of the commands in the View mode are accessible from any of the other modes with the exception of the ENABLE command.

See Table 3 on page 20 for a sample list of commands that can be accessed from the View mode and a brief description of each command. For more detailed information about the View mode commands, see Chapter 4, “View Mode Commands” on page 45.

Table 3. View Mode Commands

Command	Definition
CLEAR IP	Clears the IP routing table and the stale kernel route on the switch.
DEBUG DOT1X	Turns on debugging is turned on for the 802.1x protocol parameters.
ENABLE	Changes the command mode from the View mode to the Privilege Executive mode.
EXIT	Exits the software from the View mode. From all other modes, exits the current command mode and returns to the previous mode.
LOGOUT	Exits the software.
SHOW RUNNING-CONFIG	Displays the current switch configuration.

Privileged Executive Command Mode

The Privileged Executive command mode is the default command mode for the manager login. The commands in this mode permit you to perform system level commands such as rebooting the system, copying configuration files, and clearing statistics. The prompt changes to "Switch#" to indicate the Privileged Executive mode.

To access the View mode from the Privileged Executive mode, enter the EXIT command. To return to the Privileged Executive mode, enter the ENABLE command.

See Table 4 for a sample list of commands that can be access from the Privileged Executive command mode. For detailed information about the commands in this mode, see Chapter 5, "Privileged Executive Mode Commands" on page 67.

Table 4. Privileged Executive Command Mode Commands

Command	Description
BOOT CONFIG-FILE	Reboots the system.
CONFIGURE TERMINAL	Changes the mode to the Configuration Terminal Mode.
COPY	Uploads the configuration file to an image or configuration file.
DISABLE	Exits the Privileged Executive command mode.
PING IP	Pings an IP address to check connectivity to another system.
REBOOT	Reboots the system.
SHOW INTERFACE	Displays interface configuration and status.

Configuration Terminal Mode

The Configuration Terminal mode allows you to configure advanced system features such as broadcast storm control, SNMP, and STP. To access this mode, you must first access the Privileged Executive mode. The prompt changes to “Switch(config)#” to indicate the software has entered the Configuration Terminal mode.

See Table 5 for a sample list of commands that can be accessed from the Configuration Terminal mode. For detailed information about the commands in this mode, see the following chapters:

- Chapter 6, “Configuration Terminal Mode Commands” on page 105
- Chapter 7, “Internet Protocol (IP) Commands” on page 149
- Chapter 8, “Simple Network Management Protocol (SNMP) Commands” on page 155

Table 5. Configuration Terminal Command Mode Commands

Command	Description
ACCESS-LIST	Creates an access list.
ARP	Sets an IP address for the Address Resolution Protocol (ARP).
LINE CONSOLE	Sets the console configuration.
HOSTNAME	Sets the name of the system.
INTERFACE	Accesses the Interface Configuration command mode (you must also specify an interface).
SNMP-SERVER ENABLE	Enables an SNMP agent on the switch.
USERNAME	Sets a system user name and password.

Interface Configuration Command Mode

The Interface Configuration command mode allows you to configure features that pertain to the interfaces such as flow control and duplex mode. To access this mode, you must first access the Privileged Executive and Configuration Terminal modes, depending on your login id. For example, to access interface 1 enter the following from the Configuration Terminal mode:

```
interface xe1
```

The prompt changes to “Switch(config-if)#” to indicate the Interface Configuration mode.

After you have accessed this mode, the commands you enter apply only to the interface specified in the Configuration Terminal mode. For example, if you enter “interface xe3” in the Configuration Terminal mode, all of the subsequent commands that you enter apply to interface 3 only. To

perform interface-specific commands on another interface, specify the new interface in the Interface Configuration mode.

For a sample list of commands that can be accessed from the Interface Configuration command mode, see Table 6. For more detailed information about the commands in the Interface Configuration mode, see the following chapters:

- Chapter 9, "Interface Configuration Mode Commands" on page 171.
- Chapter 10, "IP Interface Commands" on page 209
- Chapter 11, "802.1x Access Control Commands" on page 213
- Chapter 12, "Port Configuration" on page 239
- Chapter 13, "Spanning Tree Protocol (STP) Commands" on page 243

Table 6. Interface Configuration Command Mode Commands

Commands	Description
ARP-AGEING-TIMEOUT	Set a timer for ARP on a specific interface.
DOT1X MAX-REQ	Sets the maximum number of reauthentication attempts after authentication fails.
FLOWCONTROL ON	Enables flow control and configures the flow control mode for the interface.
IP ADDRESS	Sets an IP address for the switch or specifies that the switch uses a DHCP client to obtain an IP address.
MAC-ADDRESS	Sets the MAC address for a specified interface.
SHUTDOWN	Disables an interface.
SPANNING-TREE MODE	Sets the active spanning tree protocol and enables it on the switch.
SPEED	Sets the speed and duplex mode for an interface.

Router Mode

The Router mode permits access to Layer 3 routing commands using the RIP and OSPF protocols. Access this mode through the Configuration Terminal mode with the following commands:

- ROUTER RIP
- ROUTER OSPF

When you enter either of these commands, the prompt changes to "Switch(config-router)#" to indicate the new mode.

For a sample list of RIP and OSPF commands, see Table 7. For more information about the RIP and OSPF commands, see the following chapters:

- Chapter 14, "Routing Information Protocol (RIP) Commands" on page 269
- Chapter 15, "Open Shortest Path First (OSPF) Commands" on page 311

Table 7. RIP and OSPF Commands

Commands	Description
CLEAR IP RIP ROUTE	Clears data from the RIP routing table.
DEFAULT-METRIC	Specifies the metrics assigned to redistributed routes.
HOST AREA	Specifies a stub host entry belonging to an area.
NEIGHBOR	Specifies a neighbor router.
IP OSPF COST	Specifies the cost of link-state metric in a router-LSA.
IP OSPF AUTHENTICATION-KEY	Specifies an OSPF authentication password for the neighboring routers.

VLAN Configuration Command Mode

The VLAN Configuration command mode allows you to configure commands that are applied to a VLAN interface. For instance, you can assign an IP address to a VLAN interface in this mode.

To access this mode, you must first access the View, Privileged Executive, and Configuration Terminal modes, depending on your login id. From the Configuration Terminal command mode, type the VLAN DATABASE command. The prompt changes to "Switch(config-vlan)#" to indicate the VLAN Configuration mode.

After you have accessed the VLAN Configuration mode, you enter commands that apply to specific VLANs. For a sample list of commands

that can be accessed from the VLAN Configuration command mode, see Table 8. For more detailed information about the commands in the VLAN Configuration mode, see Chapter 17, "VLAN Commands" on page 359.

Table 8. VLAN Commands

Commands	Description
SHOW VLAN	Displays information about a particular VLAN.
VLAN	Creates a VLAN and enables it.
VLAN NAME	Assigns a name to a VLAN.
VLAN STATE	Sets the operational state of the VLAN.

Line Mode Commands

To Line mode permits you to assign a console timeout, the length of the console lines, and the user privilege level when creating a Telnet connection. Access the Line mode through the Configuration Terminal mode, with the LINE VTY command. The prompt changes to "Switch(config-line)#" to indicate the Line mode.

For a list of commands that can be accessed from the Line mode, see Table 9. For more information about this mode, see Chapter 16, "Line Mode Commands" on page 355.

Table 9. Line Mode Commands

Command	Description
EXEC-TIMEOUT	Sets the interval the command interpreter waits for user input detected.
LINE CONSOLE	Sets the primary terminal line.
PRIVILEGE	Sets the access level to the AT-S83 commands.

Key Chain Mode Command

The Key Chain mode is used to assign an authentication key. Use the KEY CHAIN command to access this mode from the Configuration Terminal mode. Within this mode, you can assign a key number.

For a list of commands that can be accessed from the Key Chain mode, see Table 10. The commands in this mode are in Chapter 14, “Routing Information Protocol (RIP) Commands” on page 269.

Table 10. Key Chain Mode Commands

Command	Description
IP RIP AUTHENTICATION KEY-CHAIN	Specifies the name of the authentication key chain.
KEY	Assigns a key number.
KEY CHAIN	Accesses the Key Chain mode.

Starting the Command Line Interface

To start the command line interface, perform the following procedure:

1. Type the user id and password.

   There are two default user ids and passwords. For the system administrator login, the default user id is "manager" and the default password is "friend." For the operator login, the default user id is "operator" and the default password is "operator."

   A command line prompt is displayed in Figure 2.

```
Username:manager
Password:
(none) #
```

Figure 2. Command Line Login Screen

The default switch name is "(none)" and the pound sign (#) prompt indicates the Privileged Executive mode which is the default mode accessed by the manager login.

If you login with the operator login id, the prompt changes to "none>" to indicate the View mode.

Formatting Commands

The AT-S83 software command line interface follows the same formatting conventions for all of the command modes. There are command line interface features which apply to the general use of the command line and command syntax conventions which apply when entering the commands. See the following sections.

Command Line Interface Features

The following features are supported in the command line interface:

- Command history - Use the up and down arrow keys.
- Context-specific help - Press the question mark key, ?, to display a list of permitted parameters or all of the available commands for a particular command mode. There are two formatting options:

  – command ? - List the keywords or arguments that are required by a particular command. A space between a command and a question mark is required.

  – abbreviated command? - Provides a list of commands that begin with a particular character string. There is no space between the command and the question mark.

- Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix, for example, type “sh” and the software responds with “show.”
- Tab key - Pressing the Tab key fills in the rest of the keyword automatically. For example, typing “di” and then pressing the Tab key enters “disable” on the command line.

Command Formatting Conventions

The following formatting conventions are used in this manual:

- `screen text font` - This font illustrates the format of a command and command examples.
- ALL CAPITAL LETTERS- All capital letters indicate a parameter for you to enter.
- [ ] - Brackets indicate optional parameters.
- | - Vertical line separates parameter options for you to choose from.

Specifying an Interface

The AT-10408XP switch has eight 10G ports. Within the command line interface, specify each interface with “xe” and the number of the interface. For example, interface 3 is specified as “xe3.” For more information about the ports, see “Port Descriptions” on page 36.

Command Line Syntax Conventions

The following table describes the conventions used in the AT-S83 command interface.

Table 11. Command Line Syntax Conventions

Convention	Description	Example
A.B.C.D/M	Indicates an IP address and a subnet mask.	192.68.1.11/24
line	Indicates a line of text that accepts spaces without quotation marks.	Switch 24, San Jose, Building 4
string	Indicates a string of alphanumeric characters, including special characters such as spaces. You must place quotation marks around a value with spaces.	"Switch 24, San Jose, Building 4"
int	Indicates a whole integer.	202
IFNAME	Indicates an interface name. Specify values xe1 through xe8 and eth0.	xe3
mask	Indicates a subnet mask.	255.255.240.0
sec	Indicates seconds.	120
min	Indicates minutes.	8
trunk ID	Indicates trunk group ID.	4
VLANID	Indicates a VLAN instance (including name and VLAN identifier).	vlan3

Chapter 2

Introduction

This chapter covers the following topics:

Ethernet Technology

This section describes the Ethernet technology used by the AT-S83 software.

Fast Ethernet

The growing importance of LANs and the increasing complexity of desktop computing applications are fueling the need for high performance networks. A number of high-speed LAN technologies are proposed to provide greater bandwidth and improve client and server response times. Among them, Fast Ethernet, or 100T, provides a smooth evolution from 10T technology.

100Mbps Fast Ethernet is a standard specified by the IEEE 802.3 LAN committee. It is an extension of the 10Mbps Ethernet standard with the ability to transmit and receive data at 100Mbps, while maintaining the Carrier Sense Multiple Access with Collision Detection (CSMA/CD) Ethernet protocol.

Gigabit Ethernet Technology

Gigabit Ethernet is an extension of IEEE 802.3 Ethernet that uses the same packet structure, format, and support for CSMA/CD, protocol, full duplex, flow control, and management objects, but with a tenfold increase in theoretical throughput over 100Mbps Fast Ethernet and a one-hundred fold increase over 10Mbps Ethernet. Since it is compatible with all 10Mbps and 100Mbps Ethernet environments, Gigabit Ethernet provides a straightforward upgrade without wasting a company's existing investment in hardware, software, and trained personnel.

The increased speed and extra bandwidth offered by Gigabit Ethernet are essential to coping with the network bottlenecks that frequently develop as computers and their busses get faster and more users use applications that generate more traffic. Upgrading key components, such as your backbone and servers to Gigabit Ethernet can greatly improve network response time as well as significantly speed up the traffic between subnetworks.

Gigabit Ethernet enabled fast optical fiber connections to support video conferencing, complex imaging, and similar data-intensive applications. In addition, since data transfers occur at 10 times faster than Fast Ethernet, servers outfitted with Gigabit Ethernet NIC's are able to perform 10 times the number of operations in the same amount of time.

In addition, the phenomenal bandwidth delivered by Gigabit Ethernet is the most cost effective method to take advantage of today and tomorrow's rapidly improving switching and routing internetworking technologies.

Switching Technology

Another key development pushing the limits of Ethernet technology is in the field of switching technology. A switch bridges Ethernet packets at the MAC address level of the Ethernet protocol transmitting among connected Ethernet or Fast Ethernet LAN segments.

Switching is a cost-effective way of increasing the total network capacity available to users on a LAN. A switch increases capacity and decreases network loading by making it possible for a LAN to be divided into segments, which are not competing with each other for network transmission capacity. Therefore, the load on each segment is decreased.

The switch has a high-speed selective bridge between the individual segments. Traffic that needs to go from one segment to another (from one port to another) is automatically forwarded by the switch, without interfering with other segments (ports). This ability allows the total network capacity to be multiplied, while still maintaining the same network cabling and adapter cards.

For Fast Ethernet or Gigabit Ethernet, a switch is an effective way of eliminating the problem of chaining hubs beyond the two-repeater limit. A switch can be used to split parts of the network into different collision domains. For example, the switch can make it possible to expand a Fast Ethernet network beyond the 205 meter network diameter limit for 100TX networks. Switches supporting both traditional 10Mbps Ethernet and 100Mbps Fast Ethernet are also ideal for bridging between existing 10Mbps networks and new 100Mbps networks.

Switching LAN technology is a marked improvement over the previous generation of network bridges which were characterized by higher latencies. Routers have also been used to segment local area networks, but the cost of a router and the setup and maintenance required make routers relatively impractical. The AT-10408XP switch is an ideal solution to most kinds of LAN congestion problems.

Routing Protocol Support

The AT-S83 software supports IETF-compliant IPv4 and IPv6 versions of OSPF (Open Shortest Path First) and RIP (Routing Information Protocol). The RIP IPv4 Protocol Module supports both RIPv1 and RIPv2. In addition, OSPFv2 and OSPFv3 protocol modules are provided with IPv4 and IPv6 support.

RIP

A distance-vector protocol, RIP is an Interior Gateway Protocol (IGP) that uses hop counts as its metric. The AT-S83 software supports RIP module supports RFCs 1058 and 1723. The RIPv2 module supports more fields in the RIP packets as well as security authentication features.

At regular intervals of the routing update timer and at the time of change in the topology, the RIP router sends update messages to other routers. The listening routers update their route table with the new route, and increase

the metric value of the path by one. (This is referred to as hop count.) The router recognizes the IP-address-advertising router at the next hop, then it sends the routing updates to other routers. A maximum allowable hop count is 15. If a router reaches a metric of 16 or above, the destination is defined as unreachable. This feature avoids indefinite routing loops. The split horizon and hold down features are used to avoid propagating incorrect routing information. The route becomes invalid when the route time-out timer expires. It remains in the table until the route-flush timer expires.

OSPF

A link-state routing protocol, OSPF, is an Interior Gateway Protocol (IGP) that uses the SPF Dijsktra algorithm for the Internet. OSPF sends link-state advertisements (LSAs) to all other routers within the same hierarchical area. Data on attached interfaces, metrics used, and other variables are included in OSPF LSAs. As OSPF routers accumulate link-state data, they use the SPF algorithm to calculate the shortest path to each node.

An Autonomous System (AS) or domain is defined as a group of networks with a common routing infrastructure. OSPF can work in one AS. Or, it can receive and send routes from (or to) different AS systems. An AS system consist of areas which is a group of neighboring networks or attached hosts.

All backbone OSPF area routers use the same procedures and algorithms to maintain routing information within the backbone as any other area router. The backbone topology is invisible to all routers within an area. The individual area topologies are invisible to the backbone. Sometimes the backbone is not a contiguous area. Virtual links function as if they were direct links and are configured between backbone routers that share a link to a non backbone area.

During boot-up, an OSPF router initializes its routing-protocol-specific data structures and tables. When the lower-layer protocols with which it interfaces are functional, it sends the OSPF Hello protocol packets to find neighboring routers. A router sends Hello packets as keep-alive packets, informing other routers about its continuing functionality.

Two routers are considered adjacent when their link state databases are synchronized. Multi-access networks have more than two routers. On multi-access networks, the hello protocol chooses a designated router and a designated backup router. The designated router generates LSAs for the entire multi-access network, and reduces network traffic and the size of the topological database. The designated router also determines the adjacency of routers and the synchronization of their topological databases. The data on a router’s adjacencies or state changes are provided by periodic transmission of an LSA. Failed routers are detected, and topology is changed quickly by comparing adjacencies to link states.

Each router calculates a shortest path tree, with itself as a root, from the topological database generated from these LSAs. This shortest path tree creates a routing table.

Port Descriptions

The switch has 8 10-Gigabit ports, or interfaces, that may be used in uplinking various network devices such as PCs, hubs, and other switches to provide a gigabit Ethernet uplink in full-duplex mode. In addition, there is a 10/100/1000Base-T port and a terminal port which is used to connect to a console.

Within the software, the 8 10-Gigabit ports are accessed through the Interface mode. Within the software, these ports are referred to as interfaces. To access an interface, use the interface number prefaced by “xe.” For example, to access interface 3 specify “xe3.” See Table 12 for a list of the port names on the switch and how to refer to them in the software.

The purpose of the 10/100/1000Base-T port is twofold. It is used to make a Telnet connection to the switch. In addition, it is used to download or upload files with TFTP. You can assign the 10/100/1000Base-T port an IP address that is on a different subnet from interfaces 1 through 8. For instance, you can assign an IP address on a different subnet for this port. A subset of Interface mode commands are available on this port.

The terminal port is a console port and is it not available from the AT-S83 software.

For more information about the AT-10408XP switch, see *AT-10408XP 10-Gigabit Ethernet Switch Installation Guide.*

Table 12. AT-10408XP Switch Ports

Port Name	AT-S83 Software Name
1	xe1
2	xe2
3	xe3
4	xe4
5	xe5
6	xe6
7	xe7
8	xe8
10/100/1000Base-T	eth0
Terminal Port	not applicable

Software Features

The AT-S83 software supports the following features:

- IEEE 802.1x Port-based Network Access Control
- IEEE 802.1d Spanning Tree, IEEE 802.1w Rapid Spanning Tree, and IEEE 802.1s Multiple Spanning Tree support
- IEEE 802.1q VLAN tagging and priority
- Network Time Protocol (NTP) client support
- TFTP and Xmodem download (RFC 783/1350 TFTP)
- System Log Support
- Ping
- Telnet (client and server)
- DHCP client support
- System configuration/IP configuration
- Back pressure
- IEEE 802.3x 10/100Mbps Flow control
- IEEE 802.3z 1000Mbps Flow control
- Broadcast storm filtering support
- Remote Authentication Dial-In User Service (RADIUS) client support
- IEEE 802.1q Class of Service prioritization
- IEEE 802.1q VLAN tagging and priority
- IEEE 802.1x Port Based Network Access Control
- IEEE 802.3 10BaseT Ethernet
- IEEE 802.3ab 1000Base-T
- IEEE 802.3u 100BaseTX Ethernet
- RFC 1157 Simple Network Management Protocol (SNMP)
- RFC 2571-5 SNMPv3
- RFC 1058 Routing Information Protocol (RIP) Version 1
- RFC 1723 Routing Information Protocol (RIP)
- RFC 2082 Routing Information Protocol RIP-2 MD5 Authentication
- RFC 2453 Routing Information Protocol (RIP) and Routing Information Protocol Version 2 (RIPv2)
- RFC 1765 Open Shortest Path First (OSPF) database overflow
- RFC 2328 Open Shortest Path First version 2 (OSFPv2)
- RFC 2370 OSPF Opaque LSA option
- RFC 3101 The OSPF Not-So-Stubby Area (NSSA) Option

- RFC 3509 Alternative Implementation of OSPF Area Border Routers
- Standard CLI
- MIB support for:
  - RFC 1155 SNMP MIB Tree
  - RFC 1213 MIB-II
  - RFC 1215 TRAP MIB
  - RFC 1493 Bridge MIB
  - RFC 1573 Interface Group MIB
  - RFC 1643 Ethernet-like MIB
  - RFC 1724 Routing Information Protocol (RIP) MIB
  - RFC 1850 Open Shortest Path First version 2 (OSFPv2) MIB
  - RFC 2674 802.1Q MIB

Only the features listed above are supported.

Chapter 3

Basic Management Features

This chapter provides the following sections:

Creating User Accounts

There are two default login ids that are sent from the factory. The operator login id enables you to display the software.The password for this user id is “operator.” With this login, you access the View command mode automatically. In contrast, the manager login id permits full administrator capabilities. The password for this login id is “friend.” With this login, you access the Privileged Executive mode by default.

After your initial login to the system, assign a new user id and password. Keep the manager login id and the friend password in case you forget your password.

One of the first tasks when settings up the switch is to create user accounts. If you log in using the manager login id, you have privileged access to the switch's management software. After your initial login, define new login ids and passwords to prevent unauthorized access to the switch. Be sure to record the passwords for future reference.

To create an administrator-level account for the switch, do the following:

1. From the Privileged Executive mode, type:

   ```
   configuration terminal
   ```

   The prompt changes to “switch(config)#” to indicate the Configuration Terminal mode.

2. Use the USERNAME command to define a user name with administrator privileges and a password. For example, the following commands sets the user “nan” with administrative privileges and a password of “topsecret12:”

   ```
   username nan privilege 15 password topsecret12
   ```

3. Use the SHOW RUNNING-CONFIG command to verify the user name and password. Type:

   ```
   show running-config
   ```

Caution

CLI configuration commands only modify the running configuration file and are not saved when the switch is rebooted. To save your configuration changes in nonvolatile storage, use the COPY command. See “COPY” on page 71.

SNMP Settings

Simple Network Management Protocol (SNMP) is an OSI Layer 7 (Application Layer) designed specifically for managing and monitoring network devices. SNMP enables network management stations to read and modify the settings of gateways, routers, switches, and other network devices. Use SNMP to configure system features for proper operation, monitor performance and detect potential problems in the switch, switch group, or network.

Managed devices that support SNMP include software (referred to as an agent), which runs locally on the device.A defined set of variables (managed objects) is maintained by the SNMP agent and used to manage the device.These objects are defined in a Management Information Base (MIB), which provides a standard presentation of the information controlled by the on-board SNMP agent. SNMP defines both the format of the MIB specifications and the protocol used to access this information over the network.

The AT-10408XP supports SNMP versions 1, 2c, and 3.You can specify which version of SNMP you want to use to monitor and control the switch.The three versions of SNMP vary in the level of security provided between the management station and the network device.

In SNMP v1 and v2, user authentication is accomplished using "community strings," which function like passwords.The remote user SNMP application and the switch SNMP must use the same community string. SNMP packets from any station that has not been authenticated are ignored or dropped.

The default community strings for the switch used for SNMP v1 and v2 management access are:

- **public –** Allows authorized management stations to retrieve MIB objects.
- **private –** Allows authorized management stations to retrieve and modify MIB objects.

SNMP v3 uses a more sophisticated authentication process that is separated into two parts.The first part is to maintain a list of users and their attributes that are allowed to act as SNMP managers.The second part describes what each user on that list can do as an SNMP manager.

The switch allows groups of users to be listed and configured with a shared set of privileges.The SNMP version may also be set for a listed group of SNMP managers.Thus, you may create a group of SNMP managers that are allowed to view read-only information or receive traps using SNMP v1 while assigning a higher level of security to another group, such as granting read/write privileges using SNMP v3.

Using SNMP v3 individual users or groups of SNMP managers can be allowed to perform or be restricted from performing specific SNMP management functions.The functions allowed (or restricted) are defined using the Object Identifier (OID) associated with a specific MIB. An additional layer of security is available for SNMP v3 because SNMP messages may be encrypted. For information about how to configure SNMP v3 settings for the switch, see Chapter 8, “Simple Network Management Protocol (SNMP) Commands” on page 155.

Traps

Traps are messages that alert network personnel of events that occur on the switch.The events can be as serious as a reboot (someone accidentally turned off the switch), or less serious like a port status change.The switch generates traps and sends them to the trap recipient (or network manager).Typical traps include trap messages for Authentication Failure, Topology Change, and Broadcast/Multicast Storm.

MIBs

Management and counter information are stored by the AT-10408XP switch in the Management Information Base (MIB).The switch uses the standard MIB-II Management Information Base module. Consequently, values for MIB objects can be retrieved from any SNMP-based network management software. In addition to the standard MIB-II, the switch also supports its own proprietary enterprise MIB as an extended Management Information Base.The proprietary MIB may also be retrieved by specifying the MIB Object Identifier. MIB values can be either read-only or read-write.

Assigning an IP Address

Each switch must be assigned its own IP address, which is used for communication with an SNMP network manager or another TCP/IP application such as TFTP. (The switch does not have a default IP address.) You can change the default IP address to meet your networking address scheme. For the AT-10408XP switch, you assign IP addresses at the Interface command mode. You can assign an IP address to the 10/100/1000Base-T port as well as to each 10-Gigabit interface an IP address. In addition, you can assign the 10/100/1000Base-T port an IP address that is on a different subnet from interfaces 1 through 8. For more information about the ports, see "Port Descriptions" on page 36.

There are two ways to assign an IP address to an interface: statically and dynamically.

To assign a static IP address to an interface, use the following procedure:

1. Enter the Configuration Terminal mode, type:

   ```
   configure terminal
   ```

2. Enter the interface mode, for example, 10/100/1000Base-T port:

   ```
   interface eth0
   ```

3. Enter the IP address in the format **xxx.xxx.xxx.xxx/yyy.yyy.yyy.yyy**:

   ```
   ip 158.53.12.1/255.0.0.0
   ```

   Where the x's represent the IP address and the y's represent the corresponding subnet mask.

To assign dynamically assign an IP address to an interface, use the following procedure:

1. Enter the Configuration Terminal mode, type:

   ```
   configure terminal
   ```

2. Enter the interface mode, for example, interface 1:

   ```
   interface xe1
   ```

3. Specify DHCP:

   ```
   ip dhcp
   ```

Chapter 4

View Mode Commands

This chapter provides a description of the commands that are available from the View mode. These commands permit basic configuration of the switch. All of the following commands are also available in the Privileged Executive mode.

This chapter contains the following commands:

CLEAR ARP-CACHE

Syntax

```
clear arp-cache
```

Parameters

none

Description

Use the CLEAR ARP-CACHE command to clear all of the dynamically learned IP addresses of network devices and their corresponding MAC addresses from the Address Resolution Protocol (ARP) cache.

> **Note**
> To delete the static ARP entries, use the NO ARP command.

Command Mode

View and Privileged Executive modes

Examples

The following command clears the ARP cache:

```
switch#clear arp-cache
```

Related Commands

“ARP” on page 109

CLEAR IP

Syntax

```
clear ip mroute|ospf|pim|prefix-list|rip|route|
```

Parameters

ip — Indicates Internet Protocol parameters. Choose from the following:

- mroute — Deletes multicast route table entries.
- ospf — Clears the Open Shortest Path First (OSPF) data.
- prefix-list — Clears a prefix list.
- rip — Clears the Routing Information Protocol (RIP) information.
- route — Clears the routing table.

Description

Use the CLEAR IP command to clear the IP routing table and the stale kernel route on the switch.

Command Mode

View and Privileged Executive modes

Examples

The following command clears the IP routing table:

```
switch#clear ip rip
```

The following command clears the routing table:

```
switch#clear ip route
```

Related Commands

none

CLEAR MAC ADDRESS-TABLE

Syntax

```
clear mac address-table
```

Parameters

mac	Indicates all of the Layer-2 MAC addresses. Choose from the following:	
	dynamic	Indicates all dynamic entries.
	multicast	Indicates all multicast entries.
	static	Indicates all MAC address entries configured through the management interface.

Description

Use the CLEAR MAC command to clear the Layer-2 MAC addresses.

Command Mode

View and Privileged Executive modes

Example

The following command clears all of the dynamic Layer-2 MAC addresses:

```
switch#clear mac address-table dynamic
```

Related Commands

none

CLEAR SPANNING-TREE DETECTED PROTOCOLS

Syntax

```
clear spanning-tree detected protocols interface
IFNAME
```

Parameters

IFNAME Indicates the name of the interface.

Description

Use this command to clear the Spanning Tree parameters from the interface specified.

Command Mode

View and Privileged Executive modes

Example

The following command clears the Spanning Tree Protocol (that is STP, RSTP, or MSTP) assigned to interface 1:

```
switcheroo spanning-tree detected protocols interface
xe1
```

Related Commands

none

DEBUG DOT1X

Syntax

```
debug dot1x all|event|nsm|packet|timer

no debug dot1x all|event|nsm|packet|timer
```

Parameters

dot1x — Indicates the debugging is turned on for 802.1x protocol parameters. Choose from the following:

all	Turns on all 802.1x parameters for debugging.
event	Turns on 802.1x events for debugging.
nsm	Turns on 802.1x NSM information for debugging.
packet	Turns on 802.1x packets for debugging.
timer	Turns on 802.1x timer for debugging.

Description

Use the DEBUG DOT1X command to debug the 802.1x protocol parameters. Use the no form of this command to turn off one component of debugging.

Command Modes

View and Privileged Executive modes

Examples

The following command turns on debugging on all of the 802.1x parameters:

```
switch#debug dot1x all
```

The following command turns on debugging of the 802.1x protocol timer:

```
switch#debug dot1x timer
```

The following command turns off debugging of 802.1x packets:

```
switch#no debug dot1x packet
```

Related Commands

none

DEBUG MSTP

Syntax

```
debug mstp
```

Parameters

mstp Indicates the Multiple Spanning Tree Protocol.

all	Turns on debugging for all of the following MSTP parameters.
cli	Turns on echo commands to console feature.
packet	Turns on echo packet contents to console.
protocol	Turns on echo protocol on console.
timer	Turns on echo timer expiry to console.

Description

Use this command to debug MSTP parameters.

Command Modes

View and Privileged Executive modes

Examples

The following command debugs all of the MSTP parameters:

```
switch#debug mstp all
```

The following command displays (or echoes) MSTP commands on the console:

```
switch#debug mstp cli
```

Related Commands

none

DEBUG RIP

Syntax

```
debug rip all|events|nsm|packet
```

```
no debug all|events|nsm|packet
```

Parameters

rip — Indicates the Routing Information Protocol.

- all — Turns on debugging for all of the RIP parameters listed below.
- events — Turns on debugging for RIP events.
- nsm — Turns on debugging for NSM information.
- packet — Turns on debugging of RIP packets.

Description

Use this command to debug RIP parameters. Use the no form of this command to turn off debugging for the specified set of RIP parameters.

Command Modes

View and Privileged Executive modes

Examples

The following command debugs RIP events:

```
switch#debug rip events
```

The following command debugs RIP packets:

```
switch#debug rip packets
```

The following command turns off debugging of all RIP parameters:

```
switch#no debug rip all
```

Related Commands

none

DEBUG RSTP

Syntax

```
debug rstp
```

Parameters

rstp Indicates the Rapid Spanning Tree Protocol (RSTP).

all	Turns on debugging for all of the following RSTP parameters.
cli	Turns on echo commands to console feature.
event	Turns on echo events to console feature.
packet	Turns on echo packet contents to console.
sync	Turns on echo synchronization to console.
timer	Turns on echo timer expiry to console.

Description

Use this command to debug RSTP parameters.

Command Modes

View and Privileged Executive modes

Examples

The following command debugs all of the RSTP parameters:

```
switch#debug rstp all
```

The following command displays (or echoes) RSTP commands to the console:

```
switch#debug rstp cli
```

Related Commands

none

DEBUG SNMP

Syntax

```
debug snmp
```

Parameters

none

Use this command to debug SNMP parameters.

Command Modes

View and Privileged Executive modes

Examples

The following command turns on debugging for SNMP:

```
switch#debug snmp
```

Related Commands

none

DEBUG STP

Syntax

```
debug stp all|cli|event|packet|sync|timer
```

Parameters

stp Indicates the Spanning Tree Protocol.

all	Turns on debugging for all of the following STP parameters.
cli	Turns on echo commands to the console.
event	Turns on echo events to console.
packet	Turns on echo packet contents to the console.
protocol	Turns on protocol change to the console.
timer	Turns on echo timer expiry to the console.

Description

Use this command to access STP parameters.

Command Modes

View and Privileged Executive modes

Examples

The following command debugs all of the STP parameters:

```
switch#debug stp all
```

The following command displays (or echoes) STP commands on the console:

```
switch#debug stp cli
```

Related Commands

none

ENABLE

Syntax

```
enable
```

Parameters

none

Description

Use this command to access the Privileged Executive mode from the View mode. After you enter this command, the prompt changes to indicate you have access to the Privileged Executive mode.

Command Mode

View mode

Example

The following is an example of the ENABLE command and the Privileged Executive prompt:

```
switch>enable

switch#
```

Related Commands

none

EXIT

Syntax

```
exit
```

Parameters

none

Description

Use this command to exit the current mode and return to the previous mode. For example, if you enter this command in the Privileged Executive mode, you are returned to the View mode.

Command Mode

All modes

Example

The following is an example of the exit command:

```
switch#exit
```

Related Commands

none

HELP

Syntax

```
help
```

Parameters

none

Description

Use this command to display information about the CLI. The HELP command provides information about the current parameter. There are two forms of the HELP command:

- Full help is available when you enter a command followed by a space and the question mark (?). This displays all of the parameters for the command.
- Partial help is available when you enter an abbreviated command or argument immediately followed by the question mark (?) without a space. For example, "show con?" In this case, the software responds by displaying, "SHOW CONFIGURE."

Command Mode

All modes

Examples

The following is an example of full help and the display:

```
switch#clear ?
ip              Internet Protocol (IP)
mac             Clear layer 2 MAC entries
spanning-tree   spanning-tree
```

The following is an example of partial help and the display:

```
switch#snmp-server u?
switch#snmp-server user
```

Related Commands

none

LOGOUT

Syntax

```
logout
```

Parameters

none

Description

Use the LOGOUT command to quit the View or Privileged Executive modes and log out of the software.

Command Mode

View and Privileged Executive modes

Example

The following is an example of the LOGOUT command:

```
switch#logout
```

Related Commands

“QUIT” on page 61

QUIT

Syntax

```
quit
```

Parameters

none

Description

Use the QUIT command to quit the current mode and return to the previous mode. If you enter this command from the View or Privileged modes, you are logged out of the software.

Command Mode

All modes

Example

The following is an example of the QUIT command:

```
switch#quit
```

Related Commands

"LOGOUT" on page 60

SHOW INTERFACE SWITCHPORT

Syntax

```
show interface switchport all
```

Parameters

none

Description

Use the SHOW INTERFACE SWITCHPORT command to display the status of the 8 10-Gigabit ports.

Command Mode

View mode

Example

The following is an example of the SHOW INTERFACE SWITCHPORT command and the sample output:

```
switch#show interface switchport

Interface name:            xe1
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          2
Interface name:            xe2
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          2
Interface name:            xe3
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          3
Interface name:            xe4
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          3
```

```
Interface name:            xe5
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          3
Interface name:            xe6
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          3
Interface name:            xe7
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          3
Interface name:            xe8
Switchport mode:           access
Ingress filter:            enable
Acceptable frame types:    all
Default Vlan:              1
Configured Vlans:          3
```

Related Commands

none

SHOW RUNNING-CONFIG

Syntax

```
show running-config
```

Parameters

none

Description

Use this command to display information about the system.

Command Mode

All modes

Example

The following is an example of the SHOW RUNNING-CONFIG command and a sample of the output:

```
switch#show running-config

!
no service password-encryption
!
no service dhcp
username manager privilege 15 password friend
username operator password operator
hostname switch
!!
log trap warnings
ip domain-lookup
!
spanning-tree mode ieee
spanning-tree acquire
!
!
interface eth0
   no switchport
   shutdown
```

```
interface 1o
   mtu 0
   ip address 127.0.0.1/8
   shutdown

interface vlan1

interface xe1
   no switchport
   ip address 10.10.12.10/24
!
interface xe2
   switchport mode access
!
interface xe3
   switchport mode access
!
interface xe4
   switchport mode access
!
interface xe5
   no switchport
   ip address 10.10.10.22/24
!
interface xe6
   switchport mode access
!
interface xe7
   no switchport
   ip address 10.10.13.22/24
!
interface xe8
   switchport mode access
!
maximum-paths 8
!
snmp-server enable trap environ fan
snmp-server enable trap environ temp
snmp-server enable trap environ volt
!
   login
line vty 0 4
   login
!
end
```

Related Commands

"WRITE" on page 102

Chapter 5

Privileged Executive Mode Commands

This chapter provides a description of the commands that are available from the Privileged Executive mode. These commands permit basic configuration of the switch and access to the 802.1x protocol. In addition, you can display the current configuration of the switch. From this protocol, all of the View mode commands (with the exception of the ENABLE command) are available.

This chapter contains the following commands:

BOOT CONFIG-FILE

Syntax

```
boot config-file WORD
```

Parameters

WORD-file	Indicates the name of the boot configuration file. You must use the "-file" naming convention.

Description

Use the BOOT CONFIG-FILE command to reboot the system.

Command Mode

Privileged Executive mode

Example

The following command reboots the system with a file called "default-file:"

```
switch#boot config-file default-file
```

Related Commands

none

CONFIGURE TERMINAL

Syntax

```
configure terminal
```

Parameters

none

Description

Use this command to access the Configuration Terminal mode from the from the Privileged Executive mode. Once you access this mode, the prompt changes.

Command Mode

Privileged Executive mode

Example

The following is an example of the CONFIGURE TERMINAL command and the display of the software:

```
switch#configure terminal

switch(conf)#
```

Related Commands

none

COPY

Syntax

```
copy running-config startup-config
```

Parameters

running-config	Indicates the running configuration file.
startup-config	Indicates the start-up configuration file.

Description

Use this command to copy files. List the running configuration first then list the start-up configuration file.

Command Mode

Privileged Executive mode

Example

In the following example, the running configuration file is copied to the startup configuration file which is named "startup-config:"

```
switch#copy running-config startup-config
```

The software displays the following:

```
Building configuration...

[OK]
```

Related Commands

none

DISABLE

Syntax

```
disable
```

Parameters

none

Description

Use the DISABLE command to exit the Privileged Executive mode and return to the View mode.

To return to the Privileged Executive mode from the View mode, use the ENABLE command.

Command Mode

Privileged Executive mode

Example

The following is an example of the DISABLE command:

```
switch#disable
```

Related Commands

“ENABLE” on page 57

DOWNLOAD A.B.C.D FILE-NAME

Syntax

```
download A.B.C.D FILENAME
```

Parameters

A.B.C.D	Indicates the IP address of an TFTP server. Specify the IP address in the following format: xxx.xxx.xxx.xxx
FILENAME	Specifies a filename of a software image file.

Description

Use this command to download a software image from a TFTP server onto the switch.

Command Mode

Privileged Executive mode

Examples

The following command uses a TFTP server, with an IP address of 189.11.1.1, to download the file called "ATS83_v100.img" onto the switch:

```
switch#download 189.11.1.1 ATS83_v100.img
```

Related Commands

none

DOWNLOAD SERIAL

Syntax

```
download serial xmodem
```

Parameters

serial — Indicates the serial port. Choose from the following option:

- xmodem — Indicates the xmodem protocol is used to download a software image.

Description

Use this command to download a software image from a serial port onto the switch.

Command Mode

Privileged Executive mode

Examples

The following command uses the xmodem protocol to download the software onto the switch:

```
switch#download serial xmodem
```

Related Commands

none

DOT1X INITIALIZE

Syntax

```
dot1x initialize interface IFNAME
```

Parameters

IFNAME Specifies the name of an interface.

Description

Use this command to initialize the 802.1X Port-Based Access Control feature on a specific interface.

Command Mode

Privileged Executive mode

Example

The following command initializes the 802.1X Port-Based Access Control feature on interface 2:

```
switch#dot1x initialize interface xe2
```

Related Commands

none

PING IP

Syntax

```
ping ip WORD
```

Parameters

WORD	Specifies the hostname or an IP address in the following format: xxx.xxx.xxx.xxx

Description

This command instructs the switch to ping an end node. You can use this command to determine whether an active link exists between the switch and another network device.

Command Mode

Privileged Executive mode

Example

The following command pings an end node with the IP address of 142.245.22.22:

```
switch#ping ip 142.245.22.22
```

The results of the ping are displayed on the screen.

Related Commands

none

SHOW BOOT

Syntax

```
show boot
```

Parameters

none

Description

Use the SHOW BOOT to display information about the boot environment variables.

Command Mode

All modes

Example

The following is an example of the SHOW BOOT command and a sample display:

```
switch#show boot

Config file: /cfg/default.cfg
```

Related Commands

none

SHOW FLOWCONTROL INTERFACE

Syntax

```
show flowcontrol interface INTERFACE
```

Parameters

INTERFACE Specifies the name of an interface.

Description

Use the SHOW FLOWCONTROL INTERFACE command to display flow control information.

To modify the lines displayed on the screen, use the | (output modifier token). To save the output to a file, use the > (output reduction token).

Command Mode

Privileged Executive mode

Example

The following command displays flow control information on interface 4:

```
switch#show flowcontrol interface xe4
```

The following is a sample output of the SHOW FLOWCONTROL INTERFACE command.

Table 13. SHOW FLOWCONTROL INTERFACE Command

Port	Send	FlowControl	Receive	FlowControl	RxPause	TxPause
	admin	oper	admin	oper		
----------	----------	----------	----------	----------	----------	----------
xe1	on	on	on	on	0	0

Related Commands

none

SHOW INTERFACE

Syntax

```
show interface (IFNAME)
```

Parameters

IFNAME	Specifies the name of an interface. This is an optional parameter.

Description

Use the SHOW INTERFACE command to display the configuration and status of an interface. If you do not specify an interface, this command displays the status of all the interfaces.

Command Mode

Privileged Executive mode

Example

The following is an example of the SHOW INTERFACE command on interface 1 and the sample output:

```
switch#show interface xe1

Interface xe1
   Scope: both
   Hardware is Ethernet, address is 0004.2104.0801 (bia
004.2104.0801)
   index 2001 metric 1 mtu 1500 duplex-full arp ageing
timeout 0
   speed unknown mdix mdi
   <UP,BROADCAST,MULTICAST>
   VRF Binding: Not bound

   VRF Binding: not bound
      input packets 00, bytes 00, dropped 00, multicast
packets 00
      output packets 00, bytes 00, multicast packets 00
broadcast packets 00
```

Related Commands

none

SHOW INTERFACE STATUS ALL

Syntax

```
show interface status all
```

Parameters

none

Description

Use the SHOW INTERFACE STATUS ALL command to display the status, speed, duplex mode, and type of all the interfaces on a switch.

Command Mode

Privileged Executive mode

Example

The following example displays the command and its resulting output:

```
switch#show interface status all

Port    Name         Status      Speed    Duplex     Type
eth0    1000Base-T   connected   1000     full       unknown
xe1     interface1   connected   10G      full       XFP
xe2     interface2   connected   10G      full       XFP
xe3     interface3   connected   10G      full       XFP
xe4     interface4   connected   10G      full       XFP
xe5     interface5   connected   10G      full       XFP
xe6     interface6   connected   10G      full       XFP
xe7     interface7   connected   10G      full       XFP
xe8     interface8   connected   10G      full       XFP
```

Related Commands

“SPEED” on page 196

SHOW NTP ASSOCIATIONS DETAIL

Syntax

```
show ntp associations detail
```

Parameters

none

Description

Use the SHOW NTP ASSOCIATIONS DETAIL command to display detailed information about the Network Time Protocol (NTP).

Command Mode

All modes

Example

The following is an example of the SHOW NTP ASSOCIATIONS DETAIL command:

```
switch#show ntp associations detail

192.168.1.100 configured, sane, valid, leap_sub, stratum 16
ref ID INIT, time 00000000.00000000 ( 6:28:16.000 UTC
Fri Feb 7 2007
our mode client, peer mode unspec, our poll intvl 6,
peer poll intvl 10
root delay 0.00 msec, root disp 0.00, reach 000
delay 0.00 msec, offset 0.0000 msec, dispersion 0.00
precision 2**-20,
org time 00000000.00000000 ( 6:28:16:000 UTC Fri Feb 7 2007)
rec time 00000000.00000000 ( 6:28:16:000 UTC Fri Feb 7
2007)
xmt time 83aa7f8f.635ba2be (0:4:31:388 UTC Fri Jan 1 2007)
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 16000.00 16000.00
```

Related Commands

"SHOW NTP STATUS" on page 82

SHOW NTP STATUS

Syntax

```
show ntp status
```

Parameters

none

Description

Use the SHOW NTP STATUS command to display information about NTP.

Command Mode

All modes

Example

The following example shows the SHOW NTP STATUS command and a sample of the output:

```
switch#show ntp status

Clock is unsynchronized, stratum 16, reference is INIT
actual frequency is 0.0000 Hz, precision is 2**-19
reference time is 00000000.00000000 ( 6:28:16.000 UTC Fri
Feb 7 2007)
clock offset is 0.000msec, root delay is 0.000 msec
root dispersion is 3540.000 msec.
```

Related Commands

“SHOW NTP ASSOCIATIONS DETAIL” on page 81

SHOW STATIC-CHANNEL-GROUP

Syntax

```
show static-channel-group
```

Parameters

none

Description

Use the SHOW STATIC-CHANNEL-GROUP command to all configured static aggregators and their corresponding member ports.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW STATIC-CHANNEL-GROUP command and a sample of the output:

```
switch#show static-channel-group

% Static Aggregator: sa1
% Member:
   xe1
   xe2
   xe3
% Static Aggregator: sa2
% Member:
   xe4
```

Related Commands

none

SHOW SYSTEM STATUS

Syntax

```
show system status
```

Parameters

none

Description

Use the SHOW SYSTEM STATUS command to display information about the system power and fan status.

Command Mode

All modes

Example

The following is an example of the SHOW SYSTEM STATUS command:

```
switch#show system status

System hardware status:
System 1.25V Power..... 1.238V
System 1.8V Power ..... 1.810V
System 3.0V Power ..... 2.995V
System 3.3V Power ..... 3.300V
System 5V Power ..... 5.26V
System 12V Power ..... 11.875V
System Temperature (Celsius).. 31 C
System Fan 1 Speed ..... 4963 RPM
System Fan 2 Speed ..... 4963 RPM
System Fan 3 Speed ..... 4963 RPM
System Fan 4 Speed ..... 4921 RPM
System Fan 5 Speed ..... 4821 RPM
Main PSU Power.....On
Main PSU Temp..... Normal
Main PSU Fan..... Functional
Main PSU ..... Installed
RPS PSU Power..... Off
RPS PSU Temp..... Normal
RPS PSU Fan..... Functional
RPS PSU ..... Installed
```

Related Commands

none

SHOW VERSION

Syntax

```
show version
```

Parameters

none

Description

Use the SHOW VERSION command to display the information about the software, including:

- Version and cycle of the software
- Build date and time
- Host name
- Ethernet address

Command Mode

All modes

Example

The following example displays the command and its resulting output:

```
switch#show version
```

```
Product ID=ATS83
Application Version=1.0.0
Application Cycle=Cycle_E
Application BuildTime=19:33:00
Application BuildDate=Mar 22 2007
Loader Version=1.0.0
Loader Cycle=Cycle_A
Serial Number=None
Model=AT-10408XP
HwRev=A
Ethaddr=00:03:84:fe:d2:00
Baudrate=115200
Uptime=13:21:12 up 0 min, load average: 1.41, 0.38, 0.12
```

Related Commands

none

SYSTEM REBOOT

Syntax

```
system reboot
```

Parameters

none

Description

Use the SYSTEM REBOOT to reboot the system.

Command Mode

All modes

Example

The following is an example of the SYSTEM REBOOT command and a sample of the display:

```
switch#system reboot

The system is going down NOW!!!
Sending SIGTERM to all processes.
NSM[63]: NSM: Terminating on signal
STP[65]: STP: Terminating on signal
RSTP[67]: RSTP: Terminating on signal
MSTP[69]: MSTP: Terminating on signal
RIP[71]: RIP: Terminating on signal
OSPF[77]: OSPF: Terminating on signal
Sending SIGKILL to all processes.
Please stand by while rebooting the system.
Restarting system.
```

Related Commands

none

TELNET

Syntax

```
telnet ipaddress
```

Parameters

ipaddress	Specifies the IP address of a remote system in the following format: xxx.xxx.xxx.xxx

Description

Use this command to open a Telnet connection with a remote host. The default setting for Telnet connections is disabled.

Command Mode

Privileged Executive mode

Example

The following is an example of the TELNET command to a remote host with an IP address of 149.245.22.22:

```
switch#telnet 149.245.22.22
```

Related Commands

none

TERMINAL

Syntax

```
terminal length

no terminal length
```

Parameters

length	Specifies the number of lines that are displayed on the console. Choose a value between 0 and 512 lines.

Description

Use this command to set the number of lines on a screen or display output from a debug command.

Command Mode

Privileged Executive mode

Examples

The following command sets the number of lines on a screen to 250:

```
switch#terminal length 250
```

Related Commands

none

UNDEBUG ALL

Syntax

```
undebug all
```

Parameters

none

Description

Use the UNDEBUG ALL command to disable all of the debugging commands on the switch.

Command Mode

Privileged Executive mode

Example

The following command disables all of the debugging commands on the switch:

```
switch#undebug all
```

Related Commands

none

UNDEBUG DOT1X

Syntax

```
undebug dot1x all|event|nsm|packet|timer
```

Parameters

dot1x Indicates the IEEE 802.1x Protocol-based Access Control. Choose from the following:

all	Turns off all 802.1x parameters for debugging.
event	Indicates 802.1x events.
nsm	Indicates 802.1x NSM information.
packet	Indicates 802.1x packets.
timer	Indicates 802.1x timer.

Description

Use this command to disable 802.1x protocol debugging.

Command Modes

View and Privileged Executive modes

Examples

The following UNDEBUG 802.1x command disables debugging on all of the 802.1x parameters:

```
switch#undebug dot1x all
```

The following is an example of the UNDEBUG 802.1x command disables debugging on the 802.1x protocol timer:

```
switch#undebug dot1x timer
```

Related Commands

none

UNDEBUG OSPF EVENTS

Syntax

```
undebug ospf events abr|asbr|lsa|nssa|os|router|vlink
no undebug ospf events
```

Parameters

abr	Displays ABR events.
asbr	Displays ASBR events.
lsa	Displays Link State Advertisements (LSA) events.
nssa	Displays NSSA events.
os	Displays OS interaction events.
router	Displays other router events.
vlink	Displays virtual link events.

Description

Use the UNDEBUG OSPF EVENT command to disable the display of debug information related to OSPF internal events. Use this command without any parameters to turn on all of the options.

Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command turns on all of the OSFP debugging commands:

```
switch(config)#undebug ospf event
```

The following command displays OS interaction events on the console:

```
switch(config)#undebug ospf event os
```

Related Commands

"LOG FILE" on page 129

UNDEBUG OSPF IFSM

Syntax

```
undebug ospf ifsm status|events|timers

no undebug ifsm status|events|timers
```

Parameters

status	Displays Interface Finite State Machine (IFSM) status information.
events	Displays IFSM event information.
timers	Displays IFSM timer information.

Description

Use the UNDEBUG OPSF IFSM command to disable debugging options for OSPF IFSM. Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command disables debugging of IFSM status information:

```
switch(config)#undebug ospf ifsm status
```

The following command disables debugging of IFSM timer information:

```
switch(config)#undebug ospf ifsm timers
```

Related Commands

“LOG FILE” on page 129

UNDEBUG OSPF LSA

Syntax

```
undebug ospf lsa flooding|generate|install|maxage
|refresh

no undebug lsa status|events|timers
```

Parameters

flooding	Displays Link State Advertisements (LSA) flooding information.
generate	Displays LSA generation information.
install	Displays LSA installation information.
maxage	Displays the maximum age of the LSA in seconds.
refresh	Displays the LSA refresh information.

Description

Use the UNDEBUG OSPF LSA command to disable the display of troubleshooting information related to the internal operations of LSAs. Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command disables the display of LSA refresh information:

```
switch(config)#undebug ospf lsa refresh
```

The following command disables the display of the maximum age of the LSA:

```
switch(config)#undebug ospf lsa maxage
```

Related Commands

"LOG FILE" on page 129

UNDEBUG OSPF NFSM

Syntax

```
undebug ospf nfsm status|events|timers

no undebug nfsm status|events|timers
```

Parameters

status	Displays Neighbor Finite State Machine (NFSM) status information.
events	Displays NFSM event information.
timers	Displays NFSM timer information.

Description

Use the UNDEBUG OSPF NFSM command to disable the display of debugging information related to NFSM.

Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command disables the display of NFSM status information:

```
switch(config)#undebug ospf nfsm status
```

The following command disables the display of NFSM event information:

```
switch(config)#undebug ospf nfsm events
```

Related Commands

“LOG FILE” on page 129

UNDEBUG OSPF NSM

Syntax

```
undebug ospf nsm interface|redistribute

no undebug nsm interface|redistribute
```

Parameters

interface	Specifies NSM interface information.
redistribute	Specifies NSM redistribute information.

Description

Use the UNDEBUG OSPF NSM command to disable debugging options for OSFP NSM. Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command disables the display of NSM interface information:

```
switch(config)#undebug ospf nsm interface
```

The following command disables the display of NSM redistribute information:

```
switch(config)#undebug ospf nsm redistribute
```

Related Commands

"LOG FILE" on page 129

UNDEBUG OSPF PACKET

Syntax

```
undebug ospf packet dd|detail|hello|ls-ack
|ls-request|ls-update|recv|send

no undebug ospf packet dd|detail|hello|ls-ack
|ls-request|ls-update|recv|send
```

Parameters

dd	Specifies debugging for OSPF database information.
detail	Sets the debug option to detailed information.
hello	Specifies debugging for OSPF hello packets.
ls-ack	Specifies debugging for OSPF link-state acknowledgements.
ls-request	Specifies debugging for OSPF link-state requests.
ls-update	Specifies debugging for OSPF link-state updates.
recv	Specifies the debug option set for packets received.
send	Specifies the debug option set for packets sent.

Description

Use the DEBUG OSPF PACKET command to disable debugging options for OSFP packets. Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command disables the debug option for packets received:

```
switch(config)#undebug ospf packet recv
```

The following command disables debugging for OSPF hello packets:

```
switch(config)#undebug ospf packet hello
```

Related Commands

"LOG FILE" on page 129

UNDEBUG OSPF ROUTE

Syntax

```
undebug ospf route ase|ia|install|spf

no undebug ospf route ase|ia|install|spf
```

Parameters

ase	Specifies debugging of external route calculation information.
ia	Specifies the debugging inter-area route calculation information.
install	Specifies debugging of route installation information.
spf	Specifies the debugging of SPF calculation information.

Description

Use the UNDEBUG OSPF ROUTE command to disable debugging of route calculation. Use this command without parameters to turn on all the options.

Use the no form of this command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command disables the debug option for external route calculation information:

```
switch(config)#undebug ospf route ase
```

The following command disables debugging for inter-area route calculation information:

```
switch(config)#undebug ospf route ia
```

Related Commands

“LOG FILE” on page 129

UNDEBUG RIP

Syntax

```
undebug rip all|events|nsm|packet
```

Parameters

rip — Indicates the Routing Information Protocol. Choose from the following:

- all — Indicates all of the RIP debugging parameters.
- events — Indicates RIP events.
- nsm — Indicates NSM information.
- packet — Indicates RIP packets.

Description

Use this command to disable debugging for RIP parameters.

Command Modes

View and Privileged Executive modes

Examples

The following command disables debugging of RIP events:

```
switch#undebug rip events
```

The following command disables debugging of RIP packets:

```
switch#undebug rip packets
```

Related Commands

none

UPLOAD A.B.C.D FILE-NAME

Syntax

```
upload A.B.C.D WORD
```

Parameters

A.B.C.D	Indicates the IP address of a TFTP server. Specify the IP address in the following format: xxx.xxx.xxx.xxx
WORD	Specifies a filename.

Description

Use this command to upload a software image from the switch to a host through a TFTP server.

Command Mode

Privileged Executive mode

Example

The following command uploads image file named “ATS83.img” from the switch on to a host with an IP address of 19.11.1.1:

```
switch#upload 189.11.1.1 ATS83.img
```

Related Commands

none

UPLOAD SERIAL

Syntax

```
upload serial xmodem
```

Parameters

serial — Indicates the serial port. Choose from the following option:

- xmodem — Indicates the xmodem protocol is used to upload a software image.

Description

Use the UPLOAD SERIAL command to upload a software image from the switch onto a serial port. The serial port is also called the console port and it is labeled "TERMINAL PORT" on the switch.

Command Mode

Privileged Executive mode

Example

The following command upload the software from the switch to the serial port on the switch with the XMODEM protocol:

```
switch#upload serial xmodem
```

Related Commands

none

WRITE

Syntax

```
write file|memory|terminal
```

Parameters

file	Writes the running configuration file to another file.
memory	Writes the running configuration file to nonvolatile memory. This is an optional parameter.
terminal	Displays the running configuration file on the terminal.

Description

Use this command to write the running configuration file to memory or to another file on the network. In addition, the WRITE TERMINAL command displays the running configuration on a console. This command produces the same results as the SHOW RUNNING-CONFIG command.

The WRITE FILE command produces the same results as the COPY RUNNING_CONFIG START-UP command.

The WRITE MEMORY command produces the same results as the WRITE command.

Command Mode

Privileged Executive mode

Examples

The following example writes the running configuration file to nonvolatile memory and displays the output:

```
switch#write memory

Building configuration...

[OK]
```

The following example writes the running configuration file to the startup configuration file and displays the output:

```
switch#write file

Building configuration...
```

```
[OK]
```

The following example displays the running configuration on the terminal:

```
switch#write terminal

!
no service password-encryption
!
no service dhcp
username manager privilege 15 password friend
username operator password operator
hostname switch
!!
log trap warnings
ip domain-lookup
!
spanning-tree mode ieee
spanning-tree acquire
!
!
interface eth0
   no switchport
   shutdown

interface lo
   mtu 0
   ip address 127.0.0.1/8
   shutdown

interface vlan1
   ip address 127.0.0.2/8

interface xe1
   no switchport
   ip address 10.10.12.10/24
!
interface xe2
   switchport mode access
!
interface xe3
   switchport mode access
!
interface xe4
   switchport mode access
!
interface xe5
   no switchport
   ip address 10.10.10.22/24
!
interface xe6
   switchport mode access
!
interface xe7
```

```
   no switchport
   ip address 10.10.13.22/24
!
interface xe8
   switchport mode access
!
maximum-paths 8
!
snmp-server enable trap environ fan
snmp-server enable trap environ temp
snmp-server enable trap environ volt
!
set baudrate 115200
!
line con 0
   login local
line vty 0 15
   login local
!
end
```

Related Commands

“COPY” on page 71, “SHOW RUNNING-CONFIG” on page 64

Chapter 6

Configuration Terminal Mode Commands

The commands in this chapter are accessed through the Configuration Terminal mode. The commands in this mode allow you to configure debugging, MAC addresses, and NTP commands.

This chapter contains the following commands:

Note
The IP commands are included in the Configuration Terminal mode. They are described in Chapter 7, “Internet Protocol (IP) Commands” on page 149.

ACCESS-LIST

Syntax

```
access-list listname=word
[deny|permit|remark any|A.B.C.D/M|exact-match]
```

Parameters

LISTNAME	Indicates the name of the list. To assign attributes to the list, choose from the following options:	
	1-99	Indicates the standard IP access list.
	100-199	Indicates the extended IP access list.
	1300-1999	Indicates the expanded range of the standard IP access list.
	2000-2699	Indicates the expanded range of the extended IP access list.
deny	Specifies the packets to reject.	
permit	Specifies the route to permit packet received.	
any	Indicates packets are permitted from all routes.	
A.B.C.D/M	Indicates the IP address and subnet mask that packets can be received from.	
exact-match	Indicates the IP address and subnetmask must match the permitted or denied IP address.	
remark	Specifies a remark concerning the access list.	

Description

Use the ACCESS-LIST command to create an access list and assign it attributes. Access lists control the transmission of packets on an interface and restrict the contents of routing updates. After a match occurs between two lists, the switch stops checking. Use the ACCESS-LIST command to configure an access list for filtering packets.

When using this command from a Telnet session, make sure you Telenet to the relevant protocol daemon. For example, Telnet to isisd instead of to the Route Table Manager (RTM).

Command Mode

Configuration Terminal mode

Examples

The following commands create an access list called “mylist” and denies packets sent from IP address 10.10.0.72/24:

```
switch#configure terminal

switch(config)#access-list mylist deny 10.10.0.72/24
exact-match
```

The following commands create a file called “accesslist3” and permits packets sent from any IP address:

```
switch#configure terminal

switch(config)#access-list accesslist3 permit any
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

ARP

Syntax

```
arp A.B.C.D MAC
```

Parameters

A.B.C.D	Indicates an IP address in the following format: xxx.xxx.xxx.xxx
MAC	Indicates a MAC address in the following format: HHHH.HHHH.HHHH

Description

Use the ARP command to set an IP address for the Address Resolution Protocol.

The switch has an Address Resolution Protocol (ARP) table for storing IP addresses of network devices and their corresponding MAC addresses. The switch uses the table when you issue a management command that requires the switch's AT-S83 management software to interact with another device on the network. An example of an interaction is when you instruct the switch to ping other network devices.

To clear an IP address from the ARP table, use the CLEAR ARP-CACHE command to clear dynamic IP addresses.

Command Mode

Configuration Terminal mode

Example

The following commands add an IP address of 142.245.22.22 to the ARP table:

```
switch#configure terminal

switch(config)#arp 142.245.22.22
```

Related Commands

"CLEAR ARP-CACHE" on page 46

"SHOW RUNNING-CONFIG" on page 64

DEBUG OSPF EVENTS

Syntax

```
debug ospf events abr|asbr|lsa|nssa|os|router|vlink

no debug ospf events
```

Parameters

abr	Displays ABR events.
asbr	Displays ASBR events.
lsa	Displays Link State Advertisements (LSA) events.
nssa	Displays NSSA events.
os	Displays OS interaction events.
router	Displays other router events.
vlink	Displays virtual link events.

Description

Use the DEBUG OSPF EVENTS command to enable OSPF debugging options. The DEBUG OSPF EVENT command enables the display of debug information related to OSPF internal events. Use this command without any parameters to turn on all of the options.

Use the no form of this command or the UNDEBUG OSPF EVENT command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command enables all of the OSPF debugging options:

```
switch(config)#debug ospf events
```

The following command enables the display of OS interaction events on the console:

```
switch(config)#debug ospf events os
```

Related Commands

"LOG FILE" on page 129, "UNDEBUG OSPF EVENTS" on page 91

DEBUG OSPF IFSM

Syntax

```
debug ospf ifsm status|events|timers

no debug ifsm status|events|timers
```

Parameters

status	Displays Interface Finite State Machine (IFSM) status information.
events	Displays IFSM event information.
timers	Displays IFSM timer information.

Description

Use the DEBUG OSPF IFSM command to specify debugging options for OSPF IFSM troubleshooting information. Use the no form of this command or the UNDEBUG OSPF IFSM command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command displays IFSM status information:

```
switch(config)#debug ospf ifsm status
```

The following command displays IFSM timer information:

```
switch(config)#debug ospf ifsm timers
```

Related Commands

“LOG FILE” on page 129, “UNDEBUG OSPF IFSM” on page 92

DEBUG OSPF LSA

Syntax

```
debug ospf lsa flooding|generate|install|maxage
|refresh

no debug lsa status|events|timers
```

Parameters

flooding	Displays Link State Advertisements (LSA) flooding information.
generate	Displays LSA generation information.
install	Displays LSA installation information.
maxage	Displays the maximum age of the LSA in seconds.
refresh	Displays the LSA refresh information.

Description

Use the DEBUG OSPF LSA command to display troubleshooting information related to the internal operations of LSAs. Use the no form of this command or the UNDEBUG OSPF LSA command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command displays LSA refresh information:

```
switch(config)#debug ospf lsa refresh
```

The following command displays the maximum age of the LSA:

```
switch(config)#debug ospf lsa maxage
```

Related Commands

"LOG FILE" on page 129, "UNDEBUG OSPF LSA" on page 93

DEBUG OSPF NFSM

Syntax

```
debug ospf nfsm status|events|timers

no debug nfsm status|events|timers
```

Parameters

status	Displays OSPF Neighbor Finite State Machine (NFSM) status information.
events	Displays NFSM event information.
timers	Displays NFSM timer information.

Description

Use the DEBUG OSPF NFSM command to display debug information related to NFSM. Use the no form of this command or the UNDEBUG OSPF NFSM command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command displays NFSM status information:

```
switch(config)#debug ospf nfsm status
```

The following command displays NFSM event information:

```
switch(config)#debug ospf nfsm event
```

Related Commands

“LOG FILE” on page 129, “UNDEBUG OSPF NFSM” on page 94

DEBUG OSPF NSM

Syntax

```
debug ospf nsm interface|redistribute
```

```
no debug nsm interface|redistribute
```

Parameters

interface	Specifies NSM interface information.
redistribute	Specifies NSM redistribute information.

Description

Use the DEBUG OSPF NSM command to specify debugging options for OSFP NSM. Use the no form of this command or the UNDEBUG OSPF NSM command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command displays NSM interface information:

```
switch(config)#debug ospf nsm interface
```

The following command displays NSM redistribute information:

```
switch(config)#debug ospf nsm redistribute
```

Related Commands

"LOG FILE" on page 129, "UNDEBUG OSPF NSM" on page 95

DEBUG OSPF PACKET

Syntax

```
debug ospf packet dd|detail|hello|ls-ack
|ls-request|ls-update|recv|send

no debug ospf packet dd|detail|hello|ls-ack
|ls-request|ls-update|recv|send
```

Parameters

dd	Specifies OSPF database information.
detail	Sets the debug option to detailed information.
hello	Specifies OSPF hello packets.
ls-ack	Specifies OSPF link-state acknowledgements.
ls-request	Specifies OSPF link-state requests.
ls-update	Specifies OSPF link-state updates.
recv	Specifies received packets.
send	Specifies sent packets.

Description

Use the DEBUG OSPF PACKET command to enable debugging options for OSFP packets. Use the no form of this command or the UNDEBUG OSPF PACKET command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command enables the debug option for received packets:

```
switch(config)#debug ospf packet recv
```

The following command enables debugging for OSPF hello packets:

```
switch(config)#debug ospf packet hello
```

Related Commands

"LOG FILE" on page 129, "UNDEBUG OSPF PACKET" on page 96

DEBUG OSPF ROUTE

Syntax

```
debug ospf route ase|ia|install|spf

no debug ospf route ase|ia|install|spf
```

Parameters

ase	Specifies debugging of external route calculation.
ia	Specifies the debugging inter-area route calculation.
install	Specifies debugging of route installation.
spf	Specifies the debugging of SPF calculations.

Description

Use the DEBUG OSPF ROUTE command to specific which route calculation to debug. Use this command without parameters to turn on all of the options. Use the no form of this command or the UNDEBUG OSPF ROUTE command to disable this function.

Command Modes

Privileged Executive and Configuration Terminal modes

Examples

The following command enables the debug option for external route calculation:

```
switch(config)#debug ospf route ase
```

The following command enables debugging for SPF calculations:

```
switch(config)#debug ospf route spf
```

Related Commands

“LOG FILE” on page 129, “UNDEBUG OSPF ROUTE” on page 98

DOT1X SYSTEM-AUTH-CTRL

Syntax

```
dot1x system-auth-ctrl
```

Parameters

system-auth-ctrl Enable global interface authentication.

Description

Use the DOT1X SYSTEM-AUTH-CTRL command to enable authentication globally on interfaces 1 through 8. Global authentication is disabled by default.

Command Mode

Configuration Terminal mode

Example

The following commands enable 802.1x Port Based Access Control on all interfaces:

```
switch#configure terminal

switch(config)#dot1x system-auth-ctrl
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

ENABLE PASSWORD

Syntax

```
enable password (8) LINE
```

Parameters

8	Specifies a hidden password will follow. This is an optional parameter.
LINE	Specifies a password for the Privileged Executive Mode. Enter an alphanumeric value.

Description

This command assigns a password for the commands in the Privileged Executive mode. By default, there is no password assigned. For information about the Privileged Executive mode commands, see Chapter 5, “Privileged Executive Mode Commands” on page 67.

Command Mode

Configuration Terminal mode

Example

The following commands assign the password to “rose7:”

```
switch#configure terminal

switch(config)#enable password rose7
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

ENABLE SECRET

Syntax

```
enable secret (8) LINE
```

Parameters

8	Specifies a hidden password will follow. This is an optional parameter.
LINE	Specifies a password for the Privileged Executive Mode. Enter an alphanumeric value.

Description

This command assigns a privileged-level password, or secret. By default, there is no password assigned. For information about the Privileged Executive mode commands, see Chapter 5, "Privileged Executive Mode Commands" on page 67.

Command Mode

Configuration Terminal mode

Example

The following command assigns "aloha5551212" as the hidden password:

```
switch#configure terminal

switch(config)#enable secret 8 aloha5551212
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

EXIT

Syntax

```
exit
```

Parameters

none

Description

Use the EXIT command to quit the Configuration Terminal mode and enter the Privileged Executive mode. After you enter this command, the prompt changes to “Switchname#” to indicate the Privileged Executive mode.

Command Mode

Configuration Terminal mode

Example

The following commands exit the Configuration Terminal mode and returns the software to the Privileged Executive mode:

```
switch#configure terminal

switch(config)#exit

switch#
```

Related Commands

none

FIB RETAIN

Syntax

```
fib retain forever|time
```

Parameters

forever	Indicates the system permanently retains the FIB value.
time	Indicates time, in seconds, that the system retains FIB after RTM restarts. Specify 1 to 65535 seconds.

Description

Use the FIB RETAIN command to specify the length of time the switch retains the FIB during an RTM restart. By default, the software does not save the FIB.

Command Mode

Configuration Terminal mode

Example

The following commands retain FIB for 5,000 seconds after an RTM restart:

```
switch#configure terminal

switch(config)#fib time 5000
```

Related Commands

none

HOSTNAME

Syntax

```
hostname NAME
```

Parameters

NAME	Specifies the name of the switch. Enter a value between 1 and 63 alphanumeric characters. Names must start with a letter and end with a letter or digit. Within the interior of the name, there must only be letters, digits, and hyphens.

Description

Use the HOSTNAME command to assign a name to the switch. Enter a value between 1 and 63 alphanumeric characters. The name must follow the rules for ARPNET host names.

After you name the switch, the prompt changes to include the name. The new name of the switch appears in all of the command modes.

Command Mode

Configuration Terminal mode

Example

The following example assigns “switch” as the name of the switch and displays the new prompt:

```
none#configure terminal

none(config)#hostname switch

switch(config)#
```

Related Commands

none

INTERFACE

Syntax

```
interface
```

Parameters

IFNAME	Specifies the name of an interface.

Description

Use the INTERFACE command to access the Interface Configuration command mode for the interface specified. After you enter the INTERFACE command, "-if" is added to the prompt. For more information about the commands included in the Interface mode, see Chapter 9, "Interface Configuration Mode Commands" on page 171.

Command Mode

Configuration Terminal Mode

Examples

The following commands access the Interface mode on interface 3:

```
switch#configure terminal
switch(config)#interface xe3
switch(config-if)#
```

The following commands access the Interface mode on interface 8:

```
switch#configure terminal
switch(config)#interface xe8
switch(config-if)#
```

Related Commands

none

IP RADIUS SOURCE-INTERFACE

Syntax

```
ip radius source-interface HOSTNAME PORT

no ip radius source-interface
```

Parameters

HOSTNAME	Specifies the radius client in the dotted IP address or the hostname format.
PORT	Specifies the radius client port number. The default port number is 1812.

Description

Use the IP RADIUS SOURCE-INTERFACE command to set the local address (sent in packets) to the RADIUS client.

Use the no form of this command to clear the local address.

Command Mode

Configuration Terminal mode

Examples

The following command sets the RADIUS client to a port number of 1811.

```
switch#configure terminal

switch(config)#ip radius source-interface myhost 1811
```

Related Commands

none

LINE CONSOLE

Syntax

```
line console 0
```

Parameters

none

Description

The LINE CONSOLE command sets the console configuration and enters the Line mode. The primary terminal line is set to line number 0. After you enter this command, the prompt changes to indicate the Line mode.

For more information about the LINE mode, see Chapter 16, "Line Mode Commands" on page 355.

Command Mode

Configuration Terminal Mode

Example

The following commands set the primary line console to 0:

```
switch#configure terminal

switch(config)#line console 0

switch(config-line)#
```

Related Commands

none

LINE VTY

Syntax

```
line vty FIRST <0-15> LAST <0-15>
```

Parameters

FIRST	Specifies the first line number. Enter a value between 0 and 15.
LAST	Specifies the last line number. Enter a value between 0 and 15.

Description

Use the LINE VTY command to Telnet from the serial port to the RTM or to any protocol daemon. This command is necessary for all Telnet sessions. Before starting the daemon, add the value of the LINE VTY command to the daemon's configuration file.

After you enter the LINE VTY command, the prompt changes to indicate the software has entered the Line mode. For more information about this mode, see Chapter 16, "Line Mode Commands" on page 355.

Command Mode

Configuration Terminal mode

Example

The following commands shows the use of the LINE VTY command to enter the Line mode:

```
switch#configure terminal

switch(config)#line vty 0 15

switch(config-line)#
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

"LINE CONSOLE" on page 127

LOG FILE

Syntax

```
log file|record-priority|stdout|syslog
```

Parameters

file	Indicates logging to a file.
record-priority	Indicates the priority of the message.
stdout	Indicates logging goes to a standard output device (stdout).
syslog	Indicates logging goes to a System Log (syslog) file.

Description

Use the LOG FILE command to place limits on system logging files and the location of the log files. Use the no form of this command to revert logging to the default file. By default, the log file is written to a filename in the default directory which is usually usr/local/sbin.

Command Mode

Configuration Terminal Mode

Example

The following commands send logging information to the syslog file:

```
switch#configure terminal

switch(config)#log syslog
```

Related Commands

none

LOG TRAP

Syntax

```
log trap alerts|critical|debugging|emergencies|errors|
informational|notifications|warnings

no log trap
```

Parameters

trap — Indicates logging limits to a specified level. Choose from the following:

alerts	Turns on logging for the emergency and the alert levels.
critical	Turns on logging for the alerts, emergencies, and critical levels.
debugging	Turns on logging for all of the other levels and the debugging level. This is the most comprehensive trap level.
emergencies	Logs only the most severe messages.
errors	Turns on logging for the emergencies, alerts, critical levels. Also turns on the error level of logging.
informational	Turns on logging for the all of the levels except debugging.
notifications	Turns on logging for the emergencies, alerts, critical, errors, warnings levels. Also turns on logging for the notification level.
warnings	Turns on logging for the emergencies, alerts, critical, and errors levels. Also turns on logging for the warning level.

Description

Use the LOG TRAP command to specify system message logging levels. To the disable all of the levels of logging, use the no form of this command.

Command Mode

Configuration Terminal mode

Examples

The following example sets the log traps to the alert level:

```
switch# configure terminal
switch#(config)# log trap alerts
```

The following example turns on all of the logging levels:

```
switch# configure terminal
switch(config)# log trap debugging
```

Validation Commands

```
show running-config
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

"LOG FILE" on page 129

MAC ADDRESS-TABLE AGEING-TIME

Syntax

```
mac address-table ageing-time <10-1000000>

no mac address-table ageing-time
```

Parameters

ageing-time	Indicates the ageing time in seconds. Choose a value between 10 and 1,000,000 seconds. The default is 300 seconds.

Description

Use the MAC ADDRESS-TABLE AGEING-TIME command to specify the ageing time for an entry in a MAC address table. Use the no form to reset this parameter.

Command Mode

Configuration Terminal mode

Examples

The following example sets the ageing time to 120 seconds:

```
switch# configure terminal

switch#(config)# mac address-table ageing-time 120
```

Related Commands

none

MAC ADDRESS-TABLE STATIC DISCARD

Syntax

```
mac address-table static MMMM.MMMM.MMMM discard
interface IFNAME VLANID

no mac address-table static
```

Parameters

static — Indicates the static MAC address in the following format:

```
MMMM.MMMM.MMMM
```

IFNAME — Indicates the name of the interface.

VLANID — Indicates the VLAN interface. Enter a value between 2 and 4094. If you do not enter a value, VLAN 1 is assumed by default.

Description

Use the MAC ADDRESS-TABLE STATIC DISCARD command to delete an entry in the MAC address table. The switch forwards packets with the specified source or destination MAC address. Only unicast static addresses are supported. By default, this command is disabled. Use the no form of this command to reset it.

Command Mode

Configuration Terminal mode

Examples

The following example deletes the MAC address of "000C:6E73:2BC4" on interface 4 on VLAN 1:

```
switch# configure terminal

switch#(config)# mac address-table static
000C:6E73:2BC4 discard interface xe4
```

Related Commands

"MAC ADDRESS-TABLE STATIC FORWARD" on page 134

MAC ADDRESS-TABLE STATIC FORWARD

Syntax

```
mac address-table static MMMM.MMMM.MMMM forward
interface IFNAME VLANID

no mac address-table static
```

Parameters

static	Indicates the static MAC address in the following format: MMMM.MMMM.MMMM
IFNAME	Indicates the name of the interface.
VLANID	Indicates the VLAN interface. Enter a value between 2 and 4094. If you do not enter a value, VLAN 1 is assumed by default.

Description

The MAC ADDRESS-TABLE STATIC FORWARD command to create an entry in the MAC address table. The switch drops packets with the specified source or destination MAC address. Only unicast static addresses are supported. By default, this command is disabled. Use the no form of this command to reset it.

Command Mode

Configuration Terminal mode

Examples

The following example sets the static address to a MAC address of “000C:6E73:2BC4” on interface 3 and VLAN 2:

```
switch# configure terminal

switch#(config)# mac address-table static
000C:6E73:2BC4 forward interface xe3 vlan2
```

Related Commands

“MAC ADDRESS-TABLE STATIC DISCARD” on page 133

MAXIMUM-PATHS

Syntax

```
maximum-paths <1-10>
```

Parameters

none

Description

Use the MAXIMUM-PATH command to specify the maximum number of multipath numbers that can be installed in the Forwarding Information Base (FIB).

Command Mode

Configuration Terminal mode

Example

The following commands set the number of maximum paths of multipath numbers to 9:

```
switch#configure terminal

switch(config)#maximum-paths 9
```

Related Commands

none

NTP ACCESS-GROUP

Syntax

```
ntp access-group peer|query-only|serve|serve-only
```

Parameters

peer	Provides full access to the switch.
query-only	Provides query-only access to the switch.
serve	Provides server and query access to the switch.
serve-only	Provides server access to the switch.

Description

Use the NTP ACCESS-GROUP command to control the Network Time Protocol (NTP) access to the switch. By setting the NTP commands, you can permit the AT-S83 software to obtain the current date and time from an NTP server located on your network or on the Internet.

Command Mode

Configuration Terminal mode

Example

The following commands permit NTP server access to the switch:

```
switch#configure terminal
switch(config)#ntp access-group serve-only
```

Related Commands

none

NTP AUTHENTICATE

Syntax

```
ntp authenticate

no ntp authenticate
```

Parameters

none

Description

Use the NTP AUTHENTICATE command to enable authentication of the NTP time source. By default, this command is disabled. To disable NTP authentication on the switch, use the no form of this command.

For instructions on how to configure NTP authentication, see "Configuring NTP Authentication" on page 370.

Command Mode

Configuration Terminal mode

Example

The following commands enable authentication of the NTP time source:

```
switch#configure terminal

switch(config)#ntp authenticate
```

Related Commands

"NTP TRUSTED-KEY" on page 143

NTP AUTHENTICATION-KEY

Syntax

```
ntp authentication-key KEYNUMBER <1-4294967295>
md5 KEY

no ntp authentication-key KEYNUMBER <1-4294967295>
```

Parameters

KEYNUMBER	Specifies a key number. Choose a value between 1 and 4,294,967,295. This key indicates a trusted time source.
MD5	Indicates MD5 (message digest algorithm 5) authentication.
KEY	Specifies the name of an authentication key.

Description

Use the NTP AUTHENTICATION-KEY command to define an authentication key. If you set this command, the AT-S83 only synchronizes to a system that carries one of the authentication keys specified.

By default, this command is disabled. To remove an authentication key, use the no form of this command.

Command Mode

Configuration Terminal mode

Example

The following commands specify an authentication key of “888” and a key name of “topsecretkey:”

```
switch#configure terminal

switch(config)#ntp authentication-key 888 md5
topscretkey
```

Related Commands

“NTP AUTHENTICATE” on page 137

“NTP TRUSTED-KEY” on page 143

NTP BROADCASTDELAY

Syntax

```
ntp broadcastdelay <1-999999>
```

Parameters

none

Description

Use the NTP BROADCASTDELAY command to specify the round-trip delay between the switch and the NTP time source. The time is specified in microseconds.

Command Mode

Configuration Terminal mode

Example

The following commands set a broadcast delay of 3,000 microseconds:

```
switch#configure terminal

switch(config)#ntp broadcastdelay 3000
```

Related Commands

none

NTP MASTER

Syntax

```
ntp master <1-15>
```

Parameters

none

Description

Use the NTP MASTER command to set the NTP master clock. Select a stratum number from 1 to 15.

Command Mode

Configuration Terminal mode

Example

The following commands set an NTP master clock to stratum number 4:

```
switch#configure terminal

switch(config)#ntp master 4
```

Related Commands

“NTP PEER” on page 141, “NTP SERVER” on page 142

NTP PEER

Syntax

```
ntp peer WORD
```

Parameters

WORD	Indicates the IP address of the NTP peer. Use the following format: xxx.xxx.xxx.xxx

Description

Use the NTP PEER command to specify the IP address of the NTP peer.

Command Mode

Configuration Terminal mode

Example

The following commands set the IP address of the NTP peer to 198.11.1.1:

```
switch#configure terminal

switch(config)#ntp peer 198.11.1.1
```

Related Commands

"NTP MASTER" on page 140, "NTP SERVER" on page 142

NTP SERVER

Syntax

```
ntp server WORD
```

Parameters

WORD	Indicates the IP address of the NTP server. Use the following format: xxx.xxx.xxx.xxx

Description

Use the NTP SERVER command to specify the IP address of the NTP server.

> **Note**
> To add more than one NTP server to the switch, enter a second NTP SERVER command with another IP address.

Command Mode

Configuration Terminal mode

Example

The following example sets the IP address of the NTP server to 198.11.1.9 and shows the resulting display:

```
switch#configure terminal

switch(config)#ntp server 198.11.1.9

Translating “198.11.1.9”... [OK]
```

Related Commands

“NTP MASTER” on page 140, “NTP PEER” on page 141

NTP TRUSTED-KEY

Syntax

```
ntp trusted-key <1-4294967295>

no ntp trusted-key <1-4294967295>
```

Parameters

none

Description

Use the NTP TRUSTED-KEY command to specify a key number for a trusted time source. You must first define a key number with the NTP AUTHENTICATION-KEY command. Enter a value between 1 and 4294967295.

By default, no trusted keys are defined. To disable the authentication of a device, use the no form of this command.

Command Mode

Configuration Terminal mode

Example

The following commands set the trusted key to 222,222:

```
switch#configure terminal

switch(config)#ntp trusted-key 222222
```

Related Commands

"NTP AUTHENTICATE" on page 137

"NTP AUTHENTICATION-KEY" on page 138

ROUTE-MAP

Syntax

```
route-map WORD deny|permit <1-65535>
```

Parameters

WORD	Indicates the route map tag.
<1-65535>	Indicates the route map number.

Description

Use the ROUTE-MAP command to specify the route map tag and the route map number.

Command Mode

Configuration Terminal mode

Example

The following commands permit the route map tag called “map1” on the route-map number 999:

```
switch#configure terminal

switch(config)#route-map map1 permit 999
```

Related Commands

none

ROUTER-ID

Syntax

```
router-id A.B.C.D
```

Parameters

WORD Indicates the IP address in the following format:

xxx.xxx.xxx.xxx.

Description

Use the ROUTER-ID command to assign the IP address of a router to the switch.

Command Mode

Configuration Terminal mode

Example

The following commands assign a router with an IP address of 198.22.22.8 to the switch:

```
switch#configure terminal

switch(config)#router-id 198.22.22.8
```

Related Commands

none

UNDEBUG ALL

Syntax

```
undebug all
```

Parameters

none

Description

Use the UNDEBUG ALL command to disable all of the debugging commands on the switch.

For information about UNDEBUG commands in the Privileged Executive Mode, see Chapter 5, “Privileged Executive Mode Commands” on page 67.

Command Modes

Configuration Terminal mode

Examples

The following command disables all of the debugging commands:

```
switch(config)#undebug all
```

Related Commands

none

USERNAME

Syntax

```
username WORD privilege <1-15> password LINE
```

Parameters

WORD Specifies a user name.

privilege Specifies a user privilege level. Enter a value between 1 and 15. Values 0 to 14 provides operator privileges. Value 15 provides an administrator, or manager, privileges.

LINE Specifies a password for an administrator or manager.

Description

Use the USERNAME command to set a user name, password, and privilege level. By default, the AT-S83 software provides two USERNAME types: operator and manager. An operator login has limited access to the AT-S83 software in the View mode. This type of user has permission to perform the following commands only:

- HELP
- LOGOUT
- SHOW RUNNING SYSTEM

A manager login has permission to perform all of the AT-S83 software commands in all of the command modes.

Command Modes

Configuration Terminal mode

Examples

The following command sets the user name to "jenny," and the privilege to "15," and the password to "friend:"

```
switch(config)#username jenny privilege 15 password
friend
```

Related Commands

"ENABLE PASSWORD" on page 120

Chapter 7

Internet Protocol (IP) Commands

This chapter provides a description of the IP commands which are accessed through the Configuration Terminal mode. The IP commands apply to the entire switch.

This chapter contains the following commands:

IP DOMAIN-LIST

Syntax

```
ip domain-list WORD
```

Parameters

domain-list	Indicates a domain string. Specify in the following format:	
	WORD	Specify a domain string such as “companyname.com.”

Description

The IP DOMAIN-LIST command adds a domain name to the domain list that resides on the Domain Name Service (DNS).

Command Mode

Configuration Terminal mode

Example

The following commands add an DNS entry called “alliedtelesis.com:”

```
switch#configure terminal

switch(config)#ip domain-list alliedtelesis.com
```

Related Commands

“IP DOMAIN-LOOKUP” on page 151, “IP DOMAIN-NAME” on page 152

IP DOMAIN-LOOKUP

Syntax

```
ip domain-lookup
```

Parameters

none

Description

The IP DOMAIN-LOOKUP command enables the Domain Name Service (DNS) on the switch.

Command Mode

Configuration Terminal mode

Example

The following commands enable DNS on the switch:

```
switch#configure terminal

switch(config)#ip domain-lookup
```

Related Commands

"IP DOMAIN-LIST" on page 150, "IP DOMAIN-NAME" on page 152

IP DOMAIN-NAME

Syntax

```
ip domain-name LISTNAME
```

Parameters

domain-name — Specifies the default domain name used by the DNS. Use the following format:

- LISTNAME — Specify a domain string such as “companyname.com.”

Description

The IP DOMAIN-NAME command sets a default domain entry for the DNS.

Command Mode

Configuration Terminal mode

Example

The following commands set the default domain entry to “alliedtelesis.com:”

```
switch#configure terminal

switch(config)#ip domain-name alliedtelesis.com
```

Related Commands

“IP DOMAIN-LIST” on page 150, “IP DOMAIN-LOOKUP” on page 151

IP EXTCOMMUNITY-LIST

Syntax

```
ip extcommunity-list LIST 1-99|100-
199|expanded|standard
```

Parameters

LIST — Specify an extended community list entry. Choose from the following options:

- 1-99 — Specify a standard extended community list number.
- 100-199 — Specify an expanded extended community list number.
- expanded — Specify an expanded extended community list.
- standard — Specify a standard extended community list.

Description

Use the IP EXTCOMMUNITY-LIST command to specify an extended community list entry.

Command Mode

Configuration Terminal mode

Example

The following commands specify an extended community access list in the expanded form:

```
switch#configure terminal

switch(config)#ip extcommunity-list expanded
```

Related Commands

none

IP FORWARDING

Syntax

```
ip forwarding
```

Parameters

none

Description

Use the IP FORWARDING command to enable IP forwarding on the switch.

Command Mode

Configuration Terminal mode

Example

The following commands enable IP forwarding on the switch.

```
switch#configure terminal

switch(config)#ip forwarding
```

Related Commands

none

Chapter 8

Simple Network Management Protocol (SNMP) Commands

This chapter provides descriptions of SNMP v1, v2c and v3 commands that are accessed through the Configuration Terminal mode.

This chapter contains the following commands:

SNMP-SERVER COMMUNITY

Syntax

```
snmp-server community STRING view VIEWNAME ro|rw

no snmp-server community
```

Parameters

STRING	Specifies the name of the SNMP community. Choose an alphanumeric value between 1 and 255 characters. This name acts as a password and permits access to SNMP.
VIEWNAME	Indicates the name of a view that was defined with the SNMP-SERVER VIEW command. Choose from the following options:
	ro — Specifies the view is read-only access.
	rw — Specifies the view is read-write access.

Description

Use the SNMP-SERVER COMMUNITY command to set the name, view, and access of an SNMP community.

Use the no form of this command to remove a community string.

Command Mode

Configuration Terminal mode

Example

The following command sets the name of the SNMP community to “engineering 78” and the view to read-write access:

```
switch#snmp-server community “engineering 78” rw
```

Related Commands

“SNMP-SERVER GROUP” on page 163

“SNMP-SERVER VIEW” on page 170

SNMP-SERVER CONTACT

Syntax

```
snmp-server contact LINE

no snmp-server contact
```

Parameters

LINE	Specifies an alphanumeric string including spaces. You do not have to use quotation marks to indicate spaces. Choose a value that is between 1 and 255 characters in length.

Description

Use the SNMP-SERVER CONTACT command to set a contact person, email address, or IP address for the SNMP system. To remove a contact from the SNMP server, use the no form of this command.

Command Mode

Configuration Terminal mode

Examples

The following command sets the SNMP server contact to info@alliedtelesis.com:

```
switch#snmp-server contact info@alliedtelesis.com
```

The following command sets the SNMP server contact to "Todd Marcus:"

```
switch#snmp-server contact Todd Marcus
```

The following command sets the SNMP server contact to IP address 192.34.12.4:

```
switch#snmp-server contact 192.34.12.4
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

SNMP-SERVER ENABLE

Syntax

```
snmp-server enable

no snmp-server enable
```

Parameters

none

Description

Use the SNMP-SERVER ENABLE command to enable an SNMP agent on the switch. Use the no form of this command to disable an SNMP agent.

Command Mode

Configuration Terminal mode

Example

The following command enables an SNMP agent on the switch:

```
switch#snmp-server enable
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

SNMP-SERVER ENABLE TRAPS ENVIRON

Syntax

```
snmp-server enable traps environ fan|volt|temp

no snmp-server enable traps environ fan|volt|temp
```

Parameters

environ — Specifies the environment of the trap. Choose from the following options:

- fan — Indicates a trap is set when the fan speed is less than 3,800 Revolutions Per Minute (RPM) or greater than 6,350 RPM.
- volt — Indicates a trap is set when the voltage level is less than 0.94 volts or greater than 12.75 volts.
- temp — Indicates a trap is set when the temperature of the switch exceeds 60° C.

Description

Use the SERVER ENABLE TRAPS ENVIRON command to enable environmental traps to a host. You must enable each environmental trap individually. For example, to set traps on the fan and the power supply you must enter two commands.

Use the no form of this command to disable SNMP environment traps. You can disable SNMP environment traps individually or all at once.

Command Mode

Configuration Terminal mode

Examples

The following command sets a trap on the fan:

```
switch#snmp-server enable traps environ fan
```

The following command sets a trap on the voltage level:

```
switch#snmp-server enable traps environ volt
```

The following command disables all of the SNMP environmental traps:

```
switch#no snmp-server disable traps environ
```

The following command disables the SNMP temperature trap:

```
switch#no snmp-server enable traps environ temp
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

“SNMP-SERVER ENABLE TRAPS SNMP” on page 161

SNMP-SERVER ENABLE TRAPS SNMP

Syntax

```
snmp-server enable traps snmp link IFNAME

no snmp-server enable traps link IFNAME
```

Parameters

link	Enables link traps.
IFNAME	Specifies the name of the interface.

Description

Use the SNMP-SERVER ENABLE TRAPS SNMP command to enable SNMP traps that are sent from a specified interface on the switch to a trap host. If no interface is specified, this command enables SNMP traps on all interfaces. Use the no form of this command to disable SNMP traps.

Command Mode

Configuration Terminal mode

Examples

The following command enables the SNMP link traps on interface 7:

```
switch#snmp-server enable traps snmp link xe7
```

The following command enables the SNMP link traps on all of the interfaces:

```
switch#snmp-server enable traps snmp link
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

"SNMP-SERVER ENABLE TRAPS ENVIRON" on page 159

"SNMP-SERVER ENABLE" on page 158

SNMP-SERVER ENGINEID LOCAL

Syntax

```
snmp-server engineid local ENGINEID-STRING

no snmp-server engineid local ENGINEID-STRING
```

Parameters

LOCAL	Indicates a local copy of SNMP.
ENGINEID-STRING	Indicates the engine ID. Choose a value of up to 24 characters.

Description

Use the SNMP-SERVER ENGINEID LOCAL command to specify the switch's engine ID on the local device. The AT-S83 software converts the value to hexidecimal format automatically. By default, an SNMP engine ID is generated automatically by the software. However, it is not displayed or stored in the running configuration.

Use the no form of this command to remove the engine ID.

Command Mode

Configuration Terminal mode

Example

The following command configures an engine ID of 123456789:

```
switch#snmp-server engineid local 123456789
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

SNMP-SERVER GROUP

Syntax

```
snmp-server group GROUPNAME v1|v2c|v3 auth|noauth|priv
notify [VIEWNAME]|read [VIEWNAME]|write [VIEWNAME]

no snmp-server group GROUPNAME v1|v2c|v3
auth|noauth|priv
```

Parameters

GROUPNAME — Specifies the group name. Choose an alphanumeric value between 1 and 255 characters.

v1 — Specifies a group that uses the SNMPv1 security mode.

v2c — Specifies a group that uses the SNMPv2c security mode.

v3 — Specifies a group that uses the SNMPv3 security mode. This SNMP version provides the most security. The SNMPv3 security mode also permits the following security-level options:

- auth — Enables MD5 and SHA packet authentication for an SNMPv3 group. This is an optional parameter.
- noauth — Enables the noAuthNoPriv security level for an SNMPv3 group. This is an optional parameter.
- priv — Enables the privacy security level which is based on DES packet encryption for an SNMPv3 group. This is an optional parameter.

notify — Specifies the view that permits a user to be notified.

- VIEWNAME — Indicates a name of a view defined with the SNMP-SERVER VIEW command.

read — Specifies the view that permits the user read access.

- VIEWNAME — Indicates a name of a view defined with the SNMP-SERVER VIEW command.

write	Specifies the view that the user is allowed to read and write.	
	VIEWNAME	Indicates a name of a view defined with the SNMP-SERVER VIEW command.

Description

Use the SNMP-SERVER GROUP command to define the access rights for an SNMP group that you created with the SNMP-SERVER USER command. The SNMP-SERVER GROUP command assigns a security model and a security level to a group.

Use the no form of this command to remove an SNMP group.

Command Mode

Configuration Terminal mode

Example

The following command creates an SNMPv1 group named “marcom” with write access to a view called “internet”:

```
switch#snmp-server group marcom v1 write 1.3.6.1
```

The following command creates an SNMPv1 group named “group1” with access to a view called “nview” with notify permission:

```
switch#snmp-server group group1 v1 notify nview
```

The following command creates an SNMPv2c group named “group2” with access to a view called “wview” with write permission and a view called “nview” with notify permission:

```
switch#snmp-server group group2 v2c write wview notify
nview
```

The following command creates an SNMPv3 group named “group3” with MD5 and SHA packet authentication enabled. This group also has access to view called “wview” with write permission and a view called “nview” with notify permission:

```
switch#snmp-server group group3 v3 auth read rview
write wview notify nview
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

“SNMP-SERVER VIEW” on page 170

SNMP-SERVER HOST

Syntax

```
snmp-server host A.B.C.D informs|traps version 1|2c
COMMUNITY-STRING

no snmp-server host A.B.C.D informs|traps version 1|2c
COMMUNITY-STRING
```

Parameters

A.B.C.D	Specifies the name or the Internet address of the host.
inform	Sends SNMP inform messages to the host specified.
traps	Sends SNMP traps to the host specified.
version	Specifies the SNMP version used to send the traps. Choose from the following: 1 Indicates SNMPv1 traps. 2c Indicates SNMPv2c traps.
COMMUNITY-STRING	Specifies the password community string that is sent with the notification operation. There is no default for this parameter.

Description

Use the SNMP-SERVER HOST command to create an SNMP v1 or v2c host which is the recipient of SNMP notifications. In addition, you define which SNMP mode (v1 or v2c) the host is able to receive.

Use the no form of the command to remove one or more of the following:

- the specified host
- specific traps that the host can receive
- the community-string.

Command Mode

Configuration Terminal mode

Example

The following command to create an SNMP v2c host with an IP address of 192.34.10.1 and traps and public notification:

```
switch#snmp-server host 192.34.10.1 traps version 2c
public
```

The following command to create an SNMP v1 host with an IP address of 192.34.10.1 that receives inform messages:

```
switch#snmp-server host 192.34.10.1 inform version 1
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

SNMP-SERVER LOCATION

Syntax

```
snmp-server location SYSTEM-LOCATION

no snmp-server location
```

Parameters

SYSTEM-LOCATION	Specifies the location of the switch. Choose a value between 1 and 255 alphanumeric characters. Spaces and special characters are permitted. You do not have to use quotation marks in location names that include spaces.

Description

Use the SNMP-SERVER LOCATION command to specify the switch location. By default, a location is not configured.

Use the no form of this command to remove the location.

Command Mode

Configuration Terminal mode

Example

The following command specifies North First Street, Building 5 as the system location:

```
switch#snmp-server location North First Street,
Building 5
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64

SNMP-SERVER USER

Syntax

```
snmp-server user USERNAME GROUPNAME remote HOST udp-
port PORT <1 - 65535> v1|v2|v3 auth|encrypted md5|sha
auth-password priv des|aes priv-password

no snmp-server user USERNAME
```

Parameters

USERNAME	Specifies the name of the user.
GROUPNAME	Specifies the name of the SNMP group. The user listed in this command becomes a member of this group.
HOST	Specifies the name of the host that connects to the agent.
PORT	Specifies the UDP port. Choose a value between 1 and 65,535.
v1	Specifies the SNMPv1 security mode.
v2c	Specifies the SNMPv2c security mode.
v3	Specifies the SNMPv3 security mode.
auth	Specifies authentication is used to verify the server. If you select this parameter, you must specify an auth-password.
encryption	Enables an encrypted password. This is an optional parameter.
md5	Specifies the MD5 security mode. This is an optional parameter.
sha	Specifies the SHA security mode. This is an optional parameter.
auth-password	Specifies the SNMP authorization password.

priv	Specifies a privacy algorithm. Choose from the following: des Specifies the CBC-DES privacy algorithm. aes Specifies the AES privacy algorithm.
priv_password	Specifies the encryption algorithm password.

Description

Use the SNMP-SERVER USER command to create an SNMP user, create an SNMP group, and assign the user to an SNMP group. In addition, the SNMP-SERVER USER command maps a security mode and security name to a group name.

Use the no form of this command to remove an SNMP user from a group.

Command Mode

Configuration Terminal mode

Example

The following command adds a user called Shufen to the group called group3 which is an SNMPv3 group connected to host4:

```
switch#snmp-server user Shufen group3 host4 v3
```

The following command removes a user called Xifan:

```
switch#no snmp-server user Xifan
```

Related Commands

"SHOW RUNNING-CONFIG" on page 64,

"SNMP-SERVER GROUP" on page 163

SNMP-SERVER VIEW

Syntax

```
snmp-server view VIEWNAME WORD include|exclude

no snmp-server view
```

Parameters

VIEWNAME	Specifies the name of the user.
WORD	Specifies the MIB Tree.
include	Includes users in this view.
exclude	Excludes users from this view.

Description

Use the SNMP-SERVER VIEW command to create an SNMP view and determine if a user can access it. The MIB tree is defined by RFC 1155 Structure of Management Information. After you create a view, you can map an SNMP group to it with the SNMP-SERVER GROUP command.

Use the no form of this command to remove an SNMP view.

Command Mode

Configuration Terminal Mode

Examples

The following command creates a view called “Internet” and allows the users that are mapped to this OID to view the Internet:

```
switch#snmp-server view Internet 1.3.6.1 include
```

The following command creates a view called “sweng4” and excludes users that are mapped to this OID from viewing its contents:

```
switch#snmp-server view sweng4 1.3.6.1.4.1 exclude
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

“SNMP-SERVER GROUP” on page 163

Chapter 9

Interface Configuration Mode Commands

This chapter describes the commands in the Interface Configuration mode. Each command in this chapter applies to a specified interface on the switch.

This chapter contains the following commands:

ARP-AGEING-TIMEOUT

Syntax

```
arp-ageing-timeout <1-3000>
```

Parameters

none

Description

Use the ARP-AGEING-TIMEOUT command to set a timer for the Address Resolution Protocol (ARP) on an interface. The timer value is in seconds. The range is from 1 to 3,000 seconds.

Command Mode

Interface mode

Example

The following commands set the ARP ageing timer to 2000 seconds on interface 1:

```
switch#configure terminal

switch(config)#interface xe1

switch(config-if)#arp-ageing-timeout 2000
```

Related Commands

none

BANDWIDTH

Syntax

```
bandwidth <1-10000000>
```

Parameters

none

Description

Use the BANDWIDTH command to define the bandwidth of an interface. The range is between 1 and 10,000,000 bits.

Command Mode

Interface mode

Example

The following commands set bandwidth on interface 8 to 35,000 bits:

```
switch#configure terminal

switch(config)#interface xe8

switch(config-if)#bandwidth 35000
```

Related Commands

none

DESCRIPTION

Syntax

```
description LINE
```

Parameters

LINE	Describes the current interface. You do not need to specify quotes when using spaces.

Description

Use the DESCRIPTION command to name, or describe, the current interface.

Command Mode

Interface mode

Example

The following commands set the description to "interface 8" to describe interface 8:

```
switch#configure terminal

switch(config)#interface xe8

switch(config-if)#description interface 8
```

Related Commands

none

FLOWCONTROL BACKPRESSURE

Syntax

```
flowcontrol backpressure on|off
```

Parameters

backpressure — Specifies back-pressure flow-control in half-duplex mode. Choose from the following options.

- on — Enables back pressure.
- off — Disables back pressure.

Description

Use the FLOWCONTROL BACKPRESSURE command to enable or disable back-pressure flow-control on an interface.

Command Mode

Interface mode

Example

The following commands turns on back-pressure flow-control in half-duplex mode on the 10/100/1000Base-T port:

```
switch#configure terminal

switch(config)#interface eth0

switch(config-if)#flowcontol backpressure on
```

Related Commands

none

FLOWCONTROL RECEIVE

Syntax

```
flowcontrol receive on|off
```

Parameters

receive Specifies IEEE 802.3x flow control to receive traffic. Choose from the following options.

- on Enables flowcontrol.
- off Disables flowcontrol.

Description

Use the FLOWCONTROL RECEIVE command to enable flow control to receive traffic on an interface.

Flow control enables connected Ethernet ports (or interfaces) 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 traffic until the condition clears. When the local device detects congestion at its end, it notifies the remote device by sending a pause frame. After the remote device receives a pause frame, the remote device stops sending data packets. This prevents the loss of data packets during the congestion period.

Command Mode

Interface mode

Example

The following commands turns on flowcontrol on interface 2:

```
switch#configure terminal

switch(config)#interface xe2

switch(config-if)#flowcontol receive on
```

Related Commands

"FLOWCONTROL SEND" on page 178

FLOWCONTROL SEND

Syntax

```
flowcontrol send on|off
```

Parameters

send	Specifies IEEE 802.3x flow control to send messages. Choose from the following options.	
	on	Enables flowcontrol.
	off	Disables flowcontrol.

Description

Use the FLOWCONTROL SEND command to enable flow control to send traffic on a specified interface. To disable flow control on the specified interface, use the no form of this command.

Command Mode

Interface mode

Example

The following commands enable flowcontrol on interface 4:

```
switch#configure terminal

switch(config)#interface xe4

switch(config-if)#flowcontol send on
```

Related Commands

“FLOWCONTROL RECEIVE” on page 177

IP ACCESS-GROUP

Syntax

```
ip access-group <1-199>|<1300-2699> in|out
```

Parameters

access-group	Sets an access group. Choose from the following options:	
	1-199	Specifies a standard or extended IP access list.
	1300-2699	Specifies a standard or extended Expanded- IP-access list.
	in	Specifies inbound packets.
	out	Specifies outbound packets.

Description

Use the IP ACCESS-GROUP command to define an access group and whether it permits inbound or outbound packets.

Command Mode

Interface mode

Example

The following commands set the access group 1300 to accept inbound packets on interface 7:

```
switch#configure terminal

switch(config)#interface xe7

switch(config-if)#ip access-group 1300 in
```

Related Commands

none

IP PROXY-ARP

Syntax

```
ip proxy-arp

no ip proxy-arp
```

Parameters

none

Description

Use the IP PROXY-ARP command to enable the proxy ARP feature on an interface. Use the no form of this command to disable the proxy ARP feature on an interface.

Command Mode

Interface mode

Example

The following commands enables ARP on VLAN 1:

```
switch#configure terminal

switch(config)#interface vlan1

switch(config-if)#ip proxy-arp
```

Related Commands

none

MAC-ADDRESS

Syntax

```
mac-address HHHH:HHHH:HHHH
```

Parameters

HHHH:HHHH:HHHH Specifies a MAC address.

Description

Use the MAC-ADDRESS command to create a MAC address for a specified interface. Use the no form of this command to delete a MAC address for a specified interface.

Command Mode

Interface mode

Example

The following commands assigns the MAC address,"00C:6E73:2BC9," to interface 3:

```
switch#configure terminal

switch(config)#interface xe3

switch(config-if)#mac-address 000C:6E73:2BC9
```

Related Commands

none

MDIX

Syntax

```
mdix mdi|mdix
```

Parameters

mdi	Specifies the interface is forced to MDI mode.
mdix	Specifies the interface is forced to MDIX mode.

Description

Use the MDIX command to force an interface to the MDI or MDIX mode.

Command Mode

Interface mode

Example

The following commands force interface 7 to MDI mode:

```
switch#configure terminal
switch(config)#interface xe7
switch(config-if)#mdix mdi
```

Related Commands

none

MTU

Syntax

```
mtu <64-17940>
```

Parameters

none

Description

Use the MTU command to set the MTU value for an interface. Choose a value between 64 and 17,940.

Command Mode

Interface mode

Example

The following commands set interface 4 to an MTU value of 1700:

```
switch#configure terminal

switch(config)#interface xe4

switch(config-if)#mtu 1700
```

Related Commands

none

MULTICAST

Syntax

```
multicast

no multicast
```

Parameters

none

Description

Use the MULTICAST command to set the multicast flag to a specified interface. Use the no form of this command to disable this function.

Command Mode

Interface mode

Example

The following commands enable a multicast flag on interface 6.

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#multicast
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

SHOW CLI

Syntax

```
show cli
```

Parameters

none

Description

Use the SHOW CLI command to display the CLI tree of the Interface command mode.

Command Mode

Interface Configuration mode

Example

The following commands display the CLI tree on interface 2:

```
switch#configure terminal

switch(config)#interface xe2

switch(config-if)#show cli
```

See below for a section of the sample output of the SHOW CLI command displayed at the Interface mode.

```
+-ospf

   +-A.B.C.D

      +-authentication [no ip ospf (A.B.C.D|) authentication]

      +-authentication-key [no ip ospf (A.B.C.D|) authentication-key]

      +-cost [no ip ospf (A.B.C.D|) cost]

      +-database-filter [no ip ospf (A.B.C.D|) database-filter]

      +-hello-interval [no ip ospf (A.B.C.D|) hello-interval]

      +-message-digest-key
```

Related Commands

none

SHUTDOWN

Syntax

```
shutdown
```

Parameters

none

Description

Use the SHUTDOWN command to shut down the selected interface.

> **Note**
> There is not a no form of this command. As a result, once you shut down an interface with the SHUTDOWN command, you cannot use this command to restore or reactivate an interface.

Command Mode

Interface mode

Example

The following commands shut down interface 4:

```
switch#configure terminal
switch(config)#interface xe4
switch(config-if)#shutdown
```

Related Commands

none

SPANNING-TREE EDGEPORT

Syntax

```
spanning-tree edgeport
```

Parameters

none

Description

Use the SPANNING-TREE EDGEPORT command to enable an interface as an edgeport.

Command Mode

Interface mode

Example

The following commands enable interface 6 as an edgeport:

```
switch#configure terminal
switch(config)#interface xe6
switch(config-if)#spanning-tree edgeport
```

Related Commands

none

SPANNING-TREE FORCE-VERSION

Syntax

```
spanning-tree force-version 0|2|3

no spanning-tree force-version
```

Parameters

0 Specifies the Spanning Tree Protocol (STP).

2 Specifies the Rapid Spanning Tree Protocol (RSTP).

3 Specifies the Multiple Spanning Tree Protocol (MSTP).

none

Description

Use the SPANNING-TREE FORCE-VERSION command to select a version of the spanning tree protocol. Use the no form of this command to set the default protocol version which is STP.

Command Mode

Interface mode

Example

The following commands assign interface 6 to MSTP:

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#spanning-tree force-version 3
```

Related Commands

none

SPANNING-TREE GUARD ROOT

Syntax

```
spanning-tree guard root
```

Parameters

none

none

Description

Use the SPANNING-TREE GUARD ROOT command to disable the reception of superior BPDUs on an interface.

Command Mode

Interface mode

Example

The following commands disable the reception of superior BPDUs on interface 3:

```
switch#configure terminal

switch(config)#interface xe3

switch(config-if)#spanning-tree guard root
```

Related Commands

none

SPANNING-TREE LINK-TYPE

Syntax

```
spanning-tree link-type point-to-point|shared

no spanning-tree link-type
```

Parameters

point-to-point	Specifies the point-to-point link type on an interface.
shared	Specifies the shared link type on an interface.

Description

Use the SPANNING-TREE LINK-TYPE command to select a link type on an interface. Use the no form of this command to disable rapid transition.

Command Mode

Interface mode

Example

The following commands assign the point-to-point link type to interface 2:

```
switch#configure terminal

switch(config)#interface xe2

switch(config-if)#spanning-tree link-type point-to-
point
```

Related Commands

none

SPANNING-TREE MST INSTANCE

Syntax

```
spanning-tree mst instance <1-15>
```

Parameters

instance	Specifies the MSTP instance. Choose an ID from 1 to 15.

Description

Use the SPANNING-TREE MST INSTANCE command to associate the interface to the bridge.

Command Mode

Interface mode

Example

The following commands associates interface 3 with the bridge:

```
switch#configure terminal

switch(config)#interface xe3

switch(config-if)#spanning-tree mst instance 9
```

Related Commands

none

SPANNING-TREE PATH-COST

Syntax

```
spanning-tree path-cost <1-200000000>

no spanning-tree path-cost
```

Parameters

path-cost	Specifies the path cost. A lower path cost indicates a greater likelihood that the interface will become a root.

Description

Use the SPANNING-TREE PATH-COST command to assign a path cost to an interface. Use the no form of this command to reset the command to its default value.

Command Mode

Interface mode

Example

The following commands assigns interface 5 a path cost of 1:

```
switch#configure terminal

switch(config)#interface xe5

switch(config-if)#spanning-tree path-cost 1
```

Related Commands

none

SPANNING-TREE PORTFAST

Syntax

```
spanning-tree portfast <cr>|bpdu-filter|bpdu-guard

no spanning-tree portfast
```

Parameters

<cr>	Enables fast transitions.
bpdu-filter	Specifies the portfast bpdu-filter for the interface.
bpdu-guard	Guards the interface against reception of BPDUs.

Description

Use the SPANNING-TREE PORTFAST command to enable fast transitions on an interface. Use the no form of this command to reset the command to its default value.

Command Mode

Interface mode

Example

The following commands assigns interface 5 to a portfast bpdu-filter:

```
switch#configure terminal

switch(config)#interface xe5

switch(config-if)#spanning-tree portfast bpdu-filter
```

Related Commands

none

SPANNING-TREE PRIORITY

Syntax

```
spanning-tree priority <0-240>

no spanning-tree priority
```

Parameters

priority	Specifies the bridge priority of an interface. Enter a value from 0 to 240 in increments of 16.

Description

Use the SPANNING-TREE PRIORITY command to define interface priority. A lower priority value indicates a greater likelihood of the interface becoming a root. Use the no form of this command to reset the command to its default value.

Command Mode

Interface mode

Example

The following commands assign interface 2 with a bridge priority of 200:

```
switch#configure terminal

switch(config)#interface xe2

switch(config-if)#spanning-tree priority 200
```

Related Commands

none

SPEED

Syntax

```
speed 1000mfull|100mfull|100mhalf|10mfull|
10mhalf|auto
```

no speed

Parameters

1000mfull	Specifies the interface is forced to operate at a speed of 1,000 Mbps in full duplex mode.
100mfull	Specifies the interface is forced to operate at a speed of 100 Mbps in full duplex mode.
100mhalf	Specifies the interface is forced to operate at a speed of 100 Mbps in half duplex mode.
10mfull	Specifies the interface is forced to operate at a speed of 10 Mbps in full duplex mode.
10mhalf	Specifies the interface is forced to operate at a speed of 10 Mbps in half duplex mode.
auto	Enables auto speed and duplex configuration.

Description

Use the SPEED command to set the speed and duplex mode for interface eth0 which is labeled, “10/100/1000Base-T” on the switch. You cannot use this command to change the speed of interfaces 1 through 8. The speed for these interfaces is set to 10G in full duplex mode and you cannot change this value.

Use the no form of this command to remove the interface speed.

Command Mode

Interface mode

Example

The following commands set interface eth0 to 1,000Mbps in full-duplex mode:

```
switch#configure terminal
```

```
switch(config)#interface eth0
switch(config-if)#speed 1000mfull
```

Related Commands

none

STATIC-CHANNEL-GROUP

Syntax

```
static-channel-group channel-number <1-6>

no static-channel-group
```

Parameters

channel-number Specifies a channel number. Enter a value from 1 to 6.

Description

Use the STATIC-CHANNEL-GROUP command to add the interface to the static aggregator with the specified key. If the aggregator does not exist, it is created and the interface is added to it.

Use the no form of the STATIC-CHANNEL-GROUP command to detach the port from the static aggregator. If the port is the last member to be detached, the command deletes the static aggregator.

Command Mode

Interface mode

Example

The following commands set the channel number to 4 on interface 6:

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#static-channel-group
channel-number 4
```

Related Commands

none

STORM-CONTROL

Syntax

```
storm-control broadcast|dlf|multicast LEVEL <1-100>

no storm-control broadcast|dlf|multicast
```

Parameters

broadcast	Sets the broadcast rate limiting value for the interface.
dlf	Sets the destination lookup failure (DLF) for the interface.
multicast	Sets the multicast rate limiting value for the interface.
LEVEL	Specifies the percentage of the threshold or the percentage of the maximum speed (pps) of the interface. Enter a value between 1 and 100.

Description

Use the STORM-CONTROL command to specify the rising threshold level for broadcasting, multicast, or destination-lookup-failure traffic. The storm control action occurs when traffic reaches the level specified with the LEVEL parameter. By default, storm control is disabled.

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 an interface. Forwarding these packets can cause the network to slow down or timeout.

Use the no form of this command to disable storm control.

Command Mode

Interface mode

Example

The following commands set the broadcast rate to 30% on interface 4:

```
switch#configure terminal

switch(config)#interface xe4

switch(config-if)#storm-control broadcast level 30
```

Related Commands

none

SWITCHPORT ACCESS VLAN

Syntax

```
switchport access vlan VLANID <2-4094>

no switchport access vlan VLANID
```

Parameters

VLANID Specifies a VLAN ID. Enter a value from 2 to 4094.

Description

Use the SWITCHPORT ACCESS VLAN command to change the default VLAN for an interface. Use the no form of this command to remove a previously created VLAN with the specified VLAN ID.

> **Note**
> The default VLAN ID is 1. Do not use a VLAN ID of 1 due to interoperability issues.

Command Mode

Interface mode

Example

The following commands sets the default VLAN to 3 on interface 6:

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#switchport access vlan 3
```

Related Commands

SHOW VLAN

SWITCHPORT MODE ACCESS

Syntax

```
switchport mode access ingress-filter enable|disable

no switchport mode
```

Parameters

ingress-filter — Sets the ingress filtering for the received frames. Choose from the following options:

- enable — Sets the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.
- disable — Turns off ingress filtering to accept frames that do not meet the classification criteria. This is the default value.

Description

Use the SWITCHPORT MODE ACCESS command to set the switching characteristics of the Layer-2 interface to access mode and classify untagged frames only. Received frames are classified based on the VLAN characteristics. Then they are accepted or discarded based on the specified filtering criteria.

Use the no form of this command to reset the mode of the Layer-2 interface to the default value which is that ingress filtering is off. Also, all frames are classified and accepted.

Command Mode

Interface mode

Example

The following commands set the ingress filtering for the received frames on interface 6:

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#switchport mode access ingress-
filter enable
```

Related Commands

"SHOW VLAN" on page 361

SWITCHPORT MODE TRUNK

Syntax

```
switchport mode trunk ingress-filter enable|disable

no switchport mode
```

Parameters

ingress-filter — Sets the ingress filtering for the received frames. Choose from the following options:

- enable — Sets the ingress filtering for received frames. Received frames that cannot be classified in the previous step based on the acceptable frame type parameter (access/trunk) are discarded.
- disable — Turns off ingress filtering to accept frames that do not meet the classification criteria. This is the default value.

Description

Use the SWITCHPORT MODE TRUNK command to set the switching characteristics of the Layer-2 interface to trunk mode and specify tagged frames only. Received frames are classified based on the VLAN characteristics. Then they are accepted or discarded based on the specified filtering criteria.

Use the no form of this command to reset the mode of the Layer-2 interface to the default value which is ingress filtering is off and all frame types are classified and accepted.

Command Mode

Interface mode

Example

The following commands enable ingress filtering for received frames:

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#switchport mode trunk ingress-filter
enable
```

Related Commands

"SHOW VLAN" on page 361

SWITCHPORT TRUNK ALLOWED VLAN

Syntax

```
switchport trunk allowed vlan
add|all|none|remove|except VLANID

no switchport trunk vlan
```

Parameters

add	Add a VLAN to transmit and receive through the Layer-2 interface.
all	Allow all VLANs to transmit and receive through the Layer-2 interface.
none	Allow no VLANs to transmit and receive through the Layer-2 interface.
remove	Remove a VLAN that transmits and receives through the Layer-2 interface.
except	All VLANs, except the VLAN for which the ID is specified, are able to transmit and receive through the Layer 2 interface.
VLANID	Specifies a VLAN ID or a list of VLAN IDs. Enter a value from 2 to 4094. Set a single VLAN, VLAN range, or a VLAN list. For a VLAN range, specify the lowest VLAN, then the highest VLAN number in the range, and separate them with a hyphen. For a VLAN list, specify VLAN numbers separated by commas.

Note
Do not enter spaces between hyphens or commas when setting parameters for VLAN ranges or lists.

Description

Use the SWITCHPORT ACCESS VLAN command to change the default VLAN for an interface. Use the no form of this command to remove a previously created VLAN with the specified VLAN ID.

Command Mode

Interface mode

Examples

The following commands add a single VLAN, VLAN 2, to the member set of interface 6:

```
switch#configure terminal

switch(config)#interface xe6

switch(config)#switchport mode trunk

switch(config-if)#switchport trunk allowed vlan add 2
```

The following commands add VLANs 2 through 6 to the member set of interface 7:

```
switch#configure terminal

switch(config)#interface xe7

switch(config)#switchport mode trunk

switch(config-if)#switchport trunk allowed vlan add 2-
6
```

The following commands add a list of VLANs to the member set of interface 5:

```
switch#configure terminal

switch(config)#interface xe5

switch(config)#switchport mode trunk

switch(config-if)#switchport trunk allowed vlan add
2,3,4
```

Related Commands

"SHOW VLAN" on page 361

"SWITCHPORT MODE TRUNK" on page 204

SWITCHPORT TRUNK NATIVE

Syntax

```
switchport trunk native vlan VLANID

no switchport trunk native vlan VLANID
```

Parameters

VLANID Sets the ID of the VLAN.

Description

Use the SWITCHPORT TRUNK NATIVE command to set the native VLAN for classifying untagged traffic through the Layer 2 interface.

Use the no form of this command to remove a native VLAN. By default, the native VLAN shares the VLAN ID of 1 with the default VLAN.

Command Mode

Interface mode

Example

The following commands set the native VLAN to VLAN 2 on interface 5:

```
switch#configure terminal

switch(config)#interface xe5

switch(config-if)#switchport trunk native vlan 2
```

Related Commands

“SHOW VLAN” on page 361

Chapter 10

IP Interface Commands

The IP Interface commands are accessed through the Interface command mode. This chapter contains the following commands:

IP ACCESS-GROUP

Syntax

```
ip access-group access-list forward|in|out
```

Parameters

access-list	Sets an access list. Choose from the following options:	
	forward	Specifies forwarded packets.
	in	Specifies inbound packets.
	out	Specifies outbound packets.

Description

Use the IP ACCESS-GROUP command to set the type of packets that an access list can accept.

Command Mode

Interface mode

Example

The following commands permit interface 7 to accept forwarded packets:

```
switch#configure terminal
switch(config)#interface xe7
switch(config-if)#ip access-group access-list forward
```

Related Commands

none

IP ADDRESS

Syntax

```
ip A.B.C.D/m dhcp
```

Parameters

A.B.C.D/m	Enter an IP address and subnet mask in the following format: xxx.xxx.xxx.xxx/mask
dhcp	Indicates the switch uses a DHCP client to obtain an IP address.

Description

Use the IP ADDRESS command to set an IP address for the switch or specify that the switch uses a DHCP client to obtain an IP address.

Command Mode

Interface mode

Example

The following commands specifies the switch uses a DHCP client to obtain an IP address on interface 5:

```
switch#configure terminal

switch(config)#interface xe5

switch(config-if)#ip dhcp
```

Related Commands

none

Chapter 11

802.1x Access Control Commands

The switch implements the server side of the IEEE 802.1x Port-based and MAC-based Network Access Control. This feature allows only authorized users, or their network devices, access to network resources by establishing criteria for each interface on the switch.

For 802.1x Access Control configuration information, see “Configuring 802.1x Access Control” on page 368.

This chapter contains the following commands:

DOT1X MAX-REQ

Syntax

```
dot1x max-req <1-10>

no dot1x max-req
```

Parameters

<1-10>	Indicates the maximum number of failed Extensible Authentication Protocol (EAP) requests that are sent to the supplicant. Choose a value between 1 and 10.

Description

Use the DOT1X MAX-REQ command to set the maximum number of reauthentication attempts after authentication fails. Use the no form of this command to reset the command to its default value. The default setting is 2 attempts.

Command Mode

Interface mode

Example

The following commands set the maximum number of reauthentication attempts to 5 on interface 2:

```
switch# configure terminal

switch(config)# interface xe2

switch(config-if)# dot1x max-req 5
```

Related Commands

none

DOT1X PORT-CONTROL

Syntax

```
dot1x port-control auto|force-authorized|force-
unauthorized dir=both|in

no dot1x port-control
```

Parameters

force-authorized	Forces an interface to an authorized state.
force-unauthorized	Forces an interface to an unauthorized state.
auto	Allows a client to negotiate authentication on an interface.
dir	Specifies the packet control direction, where: both Discards receive and transmit packets from the supplicant. in Discards receive packets from the supplicant.

Description

Use the DOT1X PORT-CONTROL command to force a port state on an interface. To remove an interface from the 802.1x management, use the no form of this command.

Command Mode

Interface mode

Example

The following commands enable authentication on interface 5:

```
switch# configure terminal

switch(config)# interface xe5

switch(config-if)# dot1x port-control auto
```

Related Commands

none

DOT1X QUIET-PERIOD

Syntax

```
dot1x quiet-period <1-65535>

no dot1x quiet-period
```

Parameters

<1-65535>	Specifies the number of seconds between the retrial of authentication. Choose a value between 1 and 65,535 seconds.

Description

Use the DOT1X QUIET-PERIOD command to set the quiet-period time interval which is the amount of time the switch is in the held (or idle) state before it tries to authenticate the client again.

When a switch cannot authenticate a client, the switch remains idle for a quiet-period interval of time, then tries again. By changing the quiet-period interval, by entering a lower number than the default, the switch can provide a faster response time.

Use the no form of this command to set the configured quiet period to the default value of 60 seconds. The default value is 60 seconds.

Command Mode

Interface mode

Example

The following series of commands set the quiet-period interval to 200 seconds on interface 2:

```
switch# configure terminal

switch(config)# interface xe2

switch(config-if)# dot1x quiet-period 200
```

Related Commands

none

DOT1X REAUTHENTICATION

Syntax

```
dot1x reauthentication
```

Parameters

none

Description

Use the DOT1X REAUTHENTICATION command to enable reauthentication on an interface.

Command Mode

Interface mode

Example

The following commands enable authentication on interface 1.

```
switch# configure terminal

switch(config)# interface xe1

switch(config-if)# dot1x reauthentication
```

Related Commands

none

DOT1X REAUTHMAX

Syntax

dot1x reauthMax <1-10>

no dot1x reauthMax <1-10>

Parameters

1 -10	Maximum number of reauthentication attempts after which the port is considered unauthorized. The default number of attempts is 2.

Command Mode

Interface mode

Description

Use the DOT1X REAUTHMAX command to set the maximum number of reauthentication attempts. After the maximum number has been reached, the interface is unauthorized.

Use the no form of this command to set the reauthentication maximum to the default value of 2.

Examples

The following commands set the maximum reauthentication value to 5 on interface 3:

```
switch# configure terminal

switch(config)# interface xe3

switch(config-if)# dot1x reauthMax 5
```

The following commands set the maximum reauthentication value to its default value on interface 4:

```
switch# configure terminal

switch(config)# interface xe4

switch(config-if)# no dot1x reauthMax
```

Related Commands

none

DOT1X SYSTEM-AUTH-CTRL

Syntax

```
dot1x system-auth-ctrl
```

```
no dot1x system-auth-ctrl
```

Parameters

none

Description

Use the DOT1X SYSTEM-AUTH-CTRL command to enable global interface authentication. To disable global authentication, use the no form of this command. By default, global authentication is turned off.

Command Mode

Configure mode

Example

Use the following commands to enable global interface authentication on the switch:

```
switch# configure terminal
```

```
switch(config)# dot1x system-auth-ctrl
```

Related Commands

none

DOT1X TIMEOUT RE-AUTHPERIOD

Syntax

```
dot1x timeout re-authperiod SECS
```

Parameters

SECS	Indicates the number of seconds between reauthorization attempts. Choose a value between is from 1 to 4,294,967,295 seconds. The default value is 3,600 seconds.

Description

Use the DOT1X TIMEOUT RE-AUTHPERIOD command to specify the time, in seconds, between reauthorization attempts by the switch (the authenticator).

Command Mode

Interface mode

Example

In the following example, the reauthorization time is set to 120 seconds on interface 5:

```
switch# configure terminal

switch(config)# interface xe5

switch(config-if)# dot1x timeout re-authperiod 120
```

Related Commands

none

DOT1X TIMEOUT SERVER-TIMEOUT

Syntax

dot1x timeout server-timeout SECS <1-65535>

Parameters

SECS	Indicates the number of seconds between reauthorization attempts. The range is from 1 to 65,535 seconds. The default is 30 seconds.

Description

Use the DOT1X TIMEOUT SERVER-TIMEOUT command to set the authentication sever response timeout.

Command Mode

Interface mode

Example

The following commands set the reauthorization time on the server to 40 seconds on interface 7:

```
switch# configure terminal

switch(config)# interface xe7

switch(config-if)# dot1x timeout server-timeout 40
```

Related Commands

none

DOT1X TIMEOUT SUPP-TIMEOUT

Syntax

```
dot1x timeout supp-timeout SECS <1-65535>

no dot1x timeout supp-timeout
```

Parameters

SECS	Specifies the supplicant response timeout. The default timeout is 30 seconds. The range is from 1 to 65,535 seconds.

Description

Use the DOT1X TIMEOUT SUPP-TIMEOUT command to set the interval for a supplicant to respond. Use the no form of this command to return it to the default setting.

Command Mode

Interface mode

Example

The following commands set the supplicant timeout to 40 seconds on interface 2.

```
switch# configure terminal

switch(config)# interface xe2

switch(config-if)# dot1x timeout supp-timeout 40
```

Related Commands

none

DOT1X TIMEOUT TX-PERIOD

Syntax

```
dot1x timeout tx-period SECS <1-65535>

no dot1x timeout tx-period SECS
```

Parameters

SECS	Specify the period between successive request ID attempts. Choose a value between 1 and 65,535 seconds.

Description

Use the DOT1X TIMEOUT TX-PERIOD command to set the interval between successive attempts to request an ID. Use the no form of this command to reset the command to its default value. The default timeout is 30 seconds.

Command Mode

Interface mode

Example

The following commands set the timeout interval to 60 seconds on interface 3:

```
switch# configure terminal

switch(config)# interface xe3

switch(config-if)# dot1x timeout tx-period 60
```

Related Commands

none

IP RADIUS SOURCE-INTERFACE

Syntax

```
ip radius source-interface HOSTNAME PORT

no ip radius source-interface
```

Parameters

hostname	Specifies the radius client in the dotted IP address or the hostname format.
port	Specifies the port number of the radius client. The default port number is 1812.

Description

Use the IP RADIUS SOURCE-INTERFACE command to set the local address which is sent in packets to the Radius server. Use the no form of this command to clear the local address.

Command Mode

Configure mode

Example

The following commands set the port number of the radius client to port 1812 on a host called "myhost:"

```
switch# configure terminal

switch(config)# ip radius source-interface myhost 1812
```

Related Commands

none

RADIUS-SERVER DEADTIME

Syntax

```
radius-server deadtime <0-1440>

no radius-server timeout
```

Parameters

<0-1440>	Indicates time in minutes. Choose a value between 0 and 1,440 minutes.

Description

Use the RADIUS-SERVER DEADTIME command to set the dead time timer. There is no default value for this command. To remove the configured value, use the no form of the command.

Command Mode

Configure mode

Example

The following commands set the dead time to 6 minutes:

```
switch# configure terminal

switch(config)# radius-server deadtime 6
```

Related Commands

none

RADIUS-SERVER HOST

Syntax

```
radius-server host HOSTNAME (PORT)

no radius-server host
```

Parameters

hostname	Set radius server (in a hostname or dotted IP notation format). The default port is 1812.
port	Specifies the port number of the radius client. The default port number is 1812.

Description

Use the RADIUS-SERVER HOST command to set the RADIUS server host name and port.

Use the no form of this command to remove the defined host and port from the list of RADIUS servers. If you do not specify a value for the port, the default value of 1812 is used automatically.

Command Mode

Configure mode

Example

The following commands assign an IP address of 192.126.12.1 to the radius-server host:

```
switch# configure terminal

switch(config)# radius-server host 192.126.12.1
```

Related Commands

none

RADIUS-SERVER KEY

Syntax

```
radius-server key KEY

no radius-server key KEY
```

Parameters

KEY	The secret key shared among the radius server and the 802.1x client. Enter a value between x and y. Special characters such as “*,” “_,” and “!” are permitted.

Description

Use the RADIUS-SERVER KEY command to set the shared secret key between a Radius server and a client.

To erase the current value of the secret key, use the no form of this command. This command has no default value.

Command Mode

Configure mode

Example

The following commands set the shared secret key to “ipi:”

```
switch# configure terminal

switch(config)# radius-server key ipi
```

Related Commands

none

RADIUS-SERVER RETRANSMIT RETRIES

Syntax

```
radius-server retransmit <1-100>

no radius-server retransmit
```

Parameters

<1-100>	Specifies the number of retries. Choose a value between 1 and 100.

Description

Use the RADIUS-SERVER RETRANSMIT RETRIES command to set the number of retries between a Radius server and a client.

To reset this command to its default value, use the no form of this command. The default value is 3.

Command Mode

Configure mode

Example

The following commands set the number of retries to 18:

```
switch# configure terminal

switch(config)# radius-server retransmit 18
```

Related Commands

none

RADIUS-SERVER TIMEOUT

Syntax

```
radius-server timeout <1-1000>

no radius-server timeout
```

Parameters

<1-1000>	Specifies the time in seconds. Choose a value between 1 and 1,0000.

Description

Use the RADIUS-SERVER TIMEOUT command to specify the length of time before communication between the switch and the RADIUS host times out. To set this command to its default value, use the no form of this command. The default time is 5 seconds.

Command Mode

Configure mode

Example

The following commands set the timeout value to 120 seconds:

```
switch# configure terminal

switch(config)# radius-server timeout 120
```

Related Commands

none

SHOW DOT1X

Syntax

show dot1x

Parameters

none

Description

Use this command to display the status of the 802.1x feature on the switch.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see the Command Line Interface Environment.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW DOT1X command and the resulting display:

```
switch# show dot1x

% 802.1x authentication enabled

% Raduis server address: 192.168.1.1.1812

% Radius client address: dhcp128.ipinfusion.com.12103

% Next radius message id: 0
```

Related Commands

"SHOW DOT1X ALL" on page 232

"SHOW DOT1X INTERFACE" on page 235

SHOW DOT1X ALL

Syntax

show dot1x all

Parameters

none

Description

Use this command to display detailed 802.1x information about all of the interfaces.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see the Command Line Interface Environment.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW DOT1X ALL command and the resulting display:

```
switch# show dot1x all

% 802.1x authentication enabled

% Radius server address: 192.168.1.1.1812

% Radius client address: dhcp128.ipinfusion.com.12103

% Next radius message id: 0

% Dot1x info for interface eth1 - 3

% portEnabled: true - portControl: auto

% portStatus: unauthorized - currentId: 11

% reAuthenticate: disabled

% abort:F fail:F start:F timeout:F success:F

% PAE: state: connecting - portMode: auto

% PAE: reAuthCount: 2 - rxRespId: 0
```

```
% PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30

% BE: state: idle - reqCount: 0 - idFromServer: 0

% BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2

% CD: adminControlledDirections: in -
operControlledDirections: in

% CD: bridgeDetected: false

% KR: rxKey: false

% KT: keyAvailable: false - keyTxEnabled: false
```

Table 14 provides a description of the parameters of the SHOW DOT1X ALL and SHOW DOT1X INTERFACE commands.

Table 14. SHOW DOT1X Parameter Description

Parameter	Description
portEnabled	Indicates the interface operational status (up-true/down-false).
portControl	Indicates the current control status of the port for 802.1x control.
portStatus	Indicates the 802.1x status of the port (authorized or unauthorized).
reAuthenticate	Indicates the status of reauthentication on an interface.
reAuthPeriod	Indicates the time period of reauthentication.
Supplicant PAE related global variables:	
abort	Indicates that authentication should be aborted when this variable is set to true.
fail	Indicates failed authentication attempt when this variable is set to false.
start	Indicates authentication should be started when this variable is set to true.
timeout	Indicates an authentication attempt timed out when this variable is set to true.
success	Indicates authentication is successful when this variable is set to true.
PAE: state Current 802.1x operational state of the interface	
mode	Indicates the mode is set to 802.1x.

Table 14. SHOW DOT1X Parameter Description (Continued)

Parameter	Description
reAuthMax	Indicates the maximum number of reauthentication attempts.
BE Backend Authentication state	
state	Indicates the status of the state machine.
reqCount	Indicates the number of requests sent to the server.
suppTimeout	Indicates the supplicant timeout period.
serverTimeout	Indicates the server timeout period.
maxReq	Specifies the maximum number of requests that can be sent.
CD	Specifies the Controlled Directions State machine.
adminControlledDirections	Indicates the administrative value (Both/In).
operControlledDirections	Indicates the operational Value (Both/In).
KR	Specifies the key receive state machine.
rxKey	Indicates true when EAPOL-Key message is received by supplicant or authenticator. Indicates false when a key is transmitted.
KT	Specifies the Key Transmit State machine.
keyAvailable	Indicates false when key has been transmitted by authenticator. Indicates true when a new key is available for key exchange.
keyTxEnabled	Indicates the key transmission status.

Related Commands

“SHOW DOT1X INTERFACE” on page 235

SHOW DOT1X INTERFACE

Syntax

```
show dot1x interface IFNAME
```

Parameters

IFNAME Indicates the name of the interface.

Description

Use this command to display the state of a particular interface.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see the Command Line Interface Environment.

Command Mode

Privileged Executive mode

Example

The following command displays the state of interface 6.

```
switch# show dot1x interface xe6
```

The following is an output of the above command. See Table 14 on page 233 for a description of the command parameters.

```
% 802.1X info for interface xe6

% portEnabled: true - portControl: Force Unauthorized

% portStatus: Unauthorized - currentId: 2

% reAuthenticate: disabled

%  reAuthPeriod: 3600

%  abort:F fail:F start:F timeout:F success:F

% PAE: state: Force Unauthorized - portMode: Force
Unauthorized

% PAE: reAuthCount: 1 - rxRespId: 0

% PAE: quietPeriod: 60 - reauthMax: 2 - txPeriod: 30

BE: state: Idle - reqCount: 0 - idFromServer: 0
```

```
BE: suppTimeout: 30 - serverTimeout: 30 - maxReq: 2

CD: adminControlledDirections: in -
operControlledDirections: in

CD: bridgeDetected: false

KR: rxKey: false

KT: keyAvailable: false - keyTxEnabled: falseExample
```

Related Commands

“SHOW DOT1X ALL” on page 232

SHOW DOT1X STATISTICS INTERFACE

Syntax

show dot1x statistics interface IFNAME

Parameters

IFNAME Specifies the name of the interface.

Description

Use the SHOW DOT1X STATISTICS INTERFACE command to display the vital statistics of an interface.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see the Command Line Interface Environment.

Command Mode

Privileged Executive mode

Example

The following example shows the SHOW DOT1X STATISTICS INTERFACE and the resulting display:

```
switch# show dot1x statistics interface xe5

% Dot1x statistics for interface xe5 - 3

% EAPOL Frames Rx: 0 - EAPOL Frames Tx: 0

% EAPOL Start Frames Rx: 0 - EAPOL Logoff Frames Rx: 0

% EAP Rsp/Id Frames Rx: 0 - EAP Response Frames Rx: 0

% EAP Req/Id Frames Tx: 35 - EAP Request Frames Tx: 0

% Invalid EAPOL Frames Rx: 0 - EAP Length Error Frames Rx: 0

% EAPOL Last Frame Version Rx: 0 - EAPOL Last Frame Src:
0000.0000.0000
```

Related Commands

none

Chapter 12

Port Configuration

This chapter contains the following commands:

FLOWCONTROL OFF

Syntax

```
flowcontrol [send|receive] off
```

Parameters

send	Specifies flow control is off on the send side.
receive	Specifies flow control is off on the receive side.

Description

Use the FLOWCONTROL OFF command to disable flow control on the interface specified.

Command Mode

Interface mode

Example

The following commands disable flow control on interface 4:

```
switch# configure terminal

switch(config)# interface xe4

switch(config-if)# flowcontrol receive off
```

Related Commands

none

FLOWCONTROL ON

Syntax

```
flowcontrol [send|receive] on
```

Parameters

send	Turns on flow control on the send side.
receive	Turns on flow control on the receive side.

Description

Use the FLOWCONTROL ON command to enable flow control and configure the flow control mode for the interface.

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.

Command Mode

Interface mode

Example

The following commands enable flow control on interface 7:

```
switch# configure terminal

switch(config)# interface xe7

switch(config-if)# flowcontrol send on
```

Related Commands

none

SHOW FLOWCONTROL INTERFACE

Syntax

```
show flowcontrol interface IFNAME
```

Parameters

IFNAME Specifies the name of the interface.

Description

Use the SHOW FLOWCONTROL INTERFACE command to display flow control information on the interface specified.

Command Mode

View mode

Examples

The following example shows the SHOW FLOWCONTROL INTERFACE command and the resulting display for interface 1:

```
switch# show flowcontrol interface xe1
```

The following is a sample output of the SHOW FLOWCONTROL INTERFACE command displaying flow control information for interface 1:

```
switch# show flowcontrol interface xe1
```

Table 15. SHOW FLOWCONTROL INTERFACE Command

Port	Send	FlowControl	Receive	FlowControl	RxPause	TxPause
	admin	oper	admin	oper		
xe1	on	on	on	on	0	0

Related Commands

none

Chapter 13

Spanning Tree Protocol (STP) Commands

The commands in this chapter can be used in the Spanning Tree Protocol (STP), Rapid Spanning Tree Protocol (RSTP), and Multiple Spanning Tree Protocol (MSTP) daemons. For additional STP commands, see Chapter 9, “Interface Configuration Mode Commands” on page 171.

This chapter contains the following commands:

REGION REGION_NAME

Syntax

```
region REGION_NAME

no region
```

Parameters

REGION_NAME	Specifies the name of the MSTP region.

Description

Use the REGION REGION_NAME command to specify the name of an MSTP region on the switch.

> **Note**
> This command applies only to MSTP.

Command Mode

MST Configuration Terminal mode

Example

The following commands specify an MSTP region, called “mstp1,” on the switch:

```
switch#configure terminal

switch(config)#spanning-tree mst configuration

switch(config-mst)# region mstp1
```

Related Commands

none

REVISION REVISION_NUMBER

Syntax

```
revision revision_number <0-255>

no revision revision_number
```

Parameters

none

Description

Use the REVISION REVISION_NUMBER command to specify the revision number MSTP region on the switch.

Note
This command applies only to MSTP.

Command Mode

MST Configuration Terminal mode

Example

The following commands specify the MSTP revision number is 200:

```
switch#configure terminal

switch(config)#spanning-tree mst configuration

switch(config-mst)# revision 200
```

Related Commands

none

SHOW SPANNING-TREE

Syntax

```
show spanning-tree stp|interface|mst|mstp|rstp
```

Parameters

stp	Specifies STP information.
interface	Specifies the name of an interface.
mst	Specifies MST information.
mstp	Specifies MSTP information.
rstp	Specifies RSTP information

Description

Use the SHOW SPANNING-TREE command to display information about the Spanning Tree Protocol configuration.

To modify the lines displayed on the screen, use the | (output modifier token). To save the output to a file, use the > (output reduction token).

Command Mode

Privileged Executive mode

Example

The following commands specify the SHOW SPANNING-TREE command:

```
switch#configure terminal

switch(config)#show spanning-tree stp
```

The following is a sample output of this command for interfaces 6-8.

```
% spanning tree enabled
% root path cost 0 - priority 32768
% forward-time 15 - hello-time 2 - max-age 20 - root port 0
% root id 800000100310d0d7
% bridge id 800000100310d0d7
% hello timer 0 - tcn timer 0 - topo change timer 0
% 0 topology changes - last topology change Mon Jan 1
00:00:00 2007
% portfast bpdu-filter disabled
```

```
% portfast bpdu-guard disabled
% portfast errdisable timeout disabled
% portfast errdisable timeout interval 1 sec
%     xe8: port 2008 - id 87d8 - path cost 2000000 -
designated cost 0
%     xe8: designated port id 87d8 - state Forwarding -
priority 128
%     xe8: designated root 8000000421040803
%     xe8: designated bridge 8000000421040803
%     xe8: forward-timer 0 - hold-timer 0 - msg age timer 0
%     xe8: forward-transitions 1
%     xe8: portfast disabled
%     xe8: portfast bpdu-guard default - Current portfast
bpdu-guard off
%     xe8: portfast bpdu-filter default - Current portfast
bpdu-filter off%
      xe8: no root guard configured - Current root guard off
%

%     xe7: port 2007 - id 87d7 - path cost 20000000 -
designated cost 0
%     xe7: designated port id 87d7 - state Forwarding -
priority 128
%     xe7: designated root 8000000421040803
%     xe7: designated bridge 8000000421040803
%     xe7: forward-timer 0 - hold-timer 0 - msg age timer 0
%     xe7: forward-transitions 1
%     xe7: portfast disabled
%     xe7: portfast bpdu-guard default - Current portfast
bpdu-guard off
%     xe7: portfast bpdu-filter default - Current portfast
bpdu-filter off%
      xe7: no root guard configured - Current root guard off
%

%     xe6: port 2006 - id 87d6 - path cost 20000000 -
designated cost 0
%     xe6: designated port id 87d6 - state Forwarding -
priority 128
%     xe6: designated root 8000000421040803
%     xe6: designated bridge 8000000421040803
%     xe6: forward-timer 0 - hold-timer 0 - msg age timer 0
%     xe6: forward-transitions 1
%     xe6: portfast disabled
%     xe6: portfast bpdu-guard default - Current portfast
bpdu-guard off
%     xe6: portfast bpdu-filter default - Current portfast
bpdu-filter off%
      xe6: no root guard configured - Current root guard off
%
--More--
```

Related Commands

none

SHOW TRAFFIC-CLASS-TABLE INTERFACE

Syntax

```
show traffic-class-table interface INTERFACE
```

Parameters

INTERFACE Indicates the name of an interface.

Description

Use the SHOW TRAFFIC-CLASS-TABLE INTERFACE command to display the traffic class table.

To modify the lines displayed, use the | (output modifier token); to save the output to a file, use the > (output redirection token). For more information, see the Command Line Interface Environment.

Command Mode

Privileged Executive mode

Example

The following commands display a traffic class table on interface 1:

```
switch#configure terminal

switch(config)#show traffic-class-table interface xe1
```

The following is a sample display of this command:

User	Prio / Num Traffic Classes							
	1	2	3	4	5	6	7	8
0	0	0	0	1	1	1	1	2
1	0	0	0	0	0	0	0	0
2	0	0	0	0	0	0	0	1
3	0	0	0	1	1	2	2	3
4	0	1	1	2	2	3	3	4
5	0	1	1	2	3	4	4	5
6	0	1	2	3	4	5	5	6
7	0	0	0	2	0	0	0	0

Related Commands

none

SPANNING-TREE ACQUIRE

Syntax

```
spanning-tree acquire
```

Parameters

```
none
```

Description

Use the SPANNING-TREE ACQUIRE command to enable dynamic learning of MAC addresses.

Command Mode

Configuration Terminal mode

Example

The following commands enable dynamic learning of MAC addresses:

```
switch#configure terminal

switch(config)#spanning-tree acquire
```

Related Commands

none

SPANNING-TREE CISCO-INTEROPERABILITY

Syntax

```
spanning-tree cisco-interoperability disable|enable
```

Parameters

disable	Disables interoperability with Cisco's version of STP, RSTP, and MSTP.
enable	Enables interoperability with Cisco's version of STP, RSTP, and MSTP.

Description

Use the SPANNING-TREE CISCO-INTEROPERABILITY command to set the status of CISCO interoperability of the STP, RSTP, and MSTP protocols with the AT-S83 software.

Command Mode

Configuration Terminal mode

Example

The following commands enable CISCO interoperability of the Spanning Tree Protocols and the AT-S83 software:

```
switch#configure terminal

switch(config)#spanning-tree cisco-interoperability
```

Related Commands

none

SPANNING-TREE ERRDISABLE-TIMEOUT

Syntax

```
spanning-tree errdisable-timeout enable|interval
```

Parameters

enable	Enables the timeout mechanism for the interface to be re-enabled.
interval	Specifies an interval of time after which the interface is enabled. The default is 300 seconds.

Description

Use the SPANNING-TREE ERRDISABLE-TIMEOUT command to enable the errdisable-timeout facility, which sets a timeout for interfaces that are disabled due to the BPDU guard feature. By default, the interface is enabled after 300 seconds.

The BPDU guard feature shuts down the interface on receiving a BPDU on a BPDU-guard enabled interface. This command associates a timer with the feature such that the interface is enabled automatically without manual intervention after a set interval. This interval can be configured by the user using the bridge spanning-tree errdisable-timeout interval command.

Command Mode

Configuration Terminal mode

Example

The following commands enable the errdisable-timeout facility:

```
switch#configure terminal

switch(config)#spanning-tree errdisable-timeout enable
```

Related Commands

none

SPANNING-TREE FORWARD-TIME

Syntax

```
spanning-tree forward-time <4-30>

no spanning-tree forward-time
```

Parameters

none

Description

Use the SPANNING-TREE FORWARD-TIME command to set the time, (in seconds), after which (if this bridge is the root bridge) each interface changes to the learning and forwarding states. This value is used by all instances. To restore the default value of 15 seconds, use the no form of this command.

Command Mode

Configuration Terminal mode

Example

The following commands set the forward delay time to 20 seconds:

```
switch#configure terminal

switch(config)#spanning-tree forward-time 20
```

Related Commands

none

SPANNING-TREE HELLO-TIME

Syntax

```
spanning-tree hello-time <1-10>

no spanning-tree hello-time
```

Parameters

none

Description

Use the SPANNING-TREE HELLO-TIME command to set the hello-time, the time in seconds after which (if this bridge is the root bridge) all the bridges in a bridged LAN exchange Bridge Protocol Data Units (BPDUs). A very low value of this command leads to excessive traffic on the network, while a higher value delays the detection of topology change. This value is used by all instances.

To restore the default value of the hello time, use the no form of this command.

Command Mode

Configuration Terminal mode

Example

The following commands set the hello delay time to 9 seconds:

```
switch#configure terminal

switch(config)#spanning-tree hello-time 9
```

Related Commands

none

SPANNING-TREE MAX-AGE

Syntax

```
spanning-tree max-age <6-40>

no spanning-tree max-age
```

Parameters

none

Description

Use the SPANNING-TREE MAX-AGE command to set the max-age for a bridge. Max-age is the maximum time, in seconds, for which (if a bridge is the root bridge) a message is considered valid. This prevents the frames from looping indefinitely. This value is used by all instances.

Set the value of max-age to greater than twice the value of hello time plus one, but less than twice the value of forward delay minus one. The allowable range for max-age is 6-40 seconds. The default value is 20 seconds.

Configure this value sufficiently high, so that a frame generated by root can be propagated to the leaf nodes without exceeding the max-age.

Use the no form of this command to restore the default value of max-age.

Command Mode

Configuration Terminal mode

Example

The following commands set the max-age time for the bridge to 10 seconds:

```
switch#configure terminal

switch(config)#spanning-tree max-age 10
```

Related Commands

none

SPANNING-TREE MAX-HOPS

Syntax

```
spanning-tree max-hops <1-40>

no spanning-tree max-hops
```

Parameters

1-40	Indicates the maximum number of hops the BPDU is valid. Choose a value between 1 and 40.

Description

Use the SPANNING-TREE MAX-AGE command to specify the maximum allowed hops for a BPDU in an MST region. The value of this command is used by all instances of MST. The default number of max-hops is 20 (in an MST region).

Specifying the max hops for a BPDU prevents messages from looping indefinitely in the network. When a bridge receives a MST BPDU that has exceeded the allowed max-hops, it discards the BPDU.

To restore the default value of this command, use the no form of this command.

Command Mode

Configuration Terminal mode

Example

The following commands set the maximum hops to 9:

```
switch#configure terminal

switch(config)#spanning-tree max-hops 9
```

Related Commands

none

SPANNING-TREE MODE

Syntax

```
spanning-tree mode stp|rstp|mstp

no spanning-tree mode
```

Parameters

stp	Specifies IEEE 801.Q Spanning-tree protocol (STP).
mstp	Specifies IEEE 801.s Multiple Spanning-tree protocol (MSTP).
rstp	Specifies IEEE 801.w rapid Rapid Spanning-tree protocol (RSTP).

Description

Use the SPANNING-TREE MODE command to specify the active Spanning Tree Protocol and enable it on the switch.

Command Mode

Configuration Terminal mode

Example

The following command sets the active spanning tree mode to RSTP and enables this mode on the switch:

```
switch#configure terminal

switch(config)#spanning-tree mode rstp
```

Related Commands

none

SPANNING-TREE MST CONFIGURATION

Syntax

```
spanning-tree mst configuration
```

Parameters

none

Description

Use the SPANNING-TREE MST CONFIGURATION command to access the MSTP mode from the Configuration Terminal mode. After you enter this command, the prompt changes to “switch(config-mst) #” to indicate the software has accessed the new mode.

To return to the Configuration Terminal mode, use the EXIT command.

Command Mode

Configuration Terminal Mode

Example

The following commands access the MSTP mode on the switch:

```
switch#configure terminal

switch(config)#spanning-tree mst configure

switch(config-mst)#
```

Related Commands

none

SPANNING-TREE MST ENABLE

Syntax

```
spanning-tree mst enable

no spanning-tree mst enable
```

Parameters

enable Specifies MSTP as the active spanning-tree protocol.

Description

Use the SPANNING-TREE MST command to enable MSTP on the switch. After you have specified MSTP, all subsequent spanning tree commands apply to MSTP. To make MSTP the active spanning tree mode and enable it on the switch, use the SPANNING TREE MODE command.

Use the no form of this command to disable MSTP on the switch.

Command Mode

Configuration Terminal mode

Example

The following commands enable MSTP on the switch:

```
switch#configure terminal

switch(config)#spanning-tree mst enable
```

Related Commands

"SPANNING-TREE MODE" on page 257

SPANNING-TREE MST INSTANCE

Syntax

```
spanning-tree mst instance <1-15>

no spanning-tree mst instance
```

Parameters

instance Specifies priority for a particular instance. Choose a value between 1 and 15.

Description

Use the SPANNING-TREE MST INSTANCE command to select a priority for the specified instance. Use the no form of this command to disable a priority for the specified instance.

Command Mode

Configuration Terminal mode

Example

The following commands select a priority of 4 for an instance:

```
switch#configure terminal

switch(config)#spanning-tree mst instance 4
```

Related Commands

none

SPANNING-TREE PORTFAST BPDU-FILTER

Syntax

```
spanning-tree portfast bpdu-filter

no spanning-tree portfast bpdu-filter
```

Parameters

none

Description

Use the Use the SPANNING-TREE BPDU-FILTER command to set a portfast BPDU filter for the bridge. Interfaces that are set to the default value take the same value of the BPDU filter as that of the bridge.

The Spanning Tree Protocol sends BPDUs from all interfaces. Enabling the BPDU Filter feature ensures that portfast-enabled interfaces do not transmit or receive any BPDUs.

Use the SHOW SPANNING-TREE command to display the configured and currently running values of the BPDU-filter parameter for the bridge and interface.

Use the no form of this command to disable the BPDU filter for the bridge.

Command Mode

Configuration Terminal mode

Example

The following commands set the PortFast BPDU filter for the bridge:

```
switch#configure terminal

switch(config)#spanning-tree portfast bpdu-filter
```

Related Commands

none

SPANNING-TREE PORTFAST BPDU-GUARD

Syntax

```
spanning-tree portfast bpdu-guard

no spanning-tree portfast bpdu-guard
```

Parameters

none

Description

Use the SPANNING-TREE BPDU-GUARD command to enable the BPDU (Bridge Protocol Data Unit) guard feature on a bridge.

When the BPDU guard feature is set for a bridge, all portfast-enabled interfaces of the bridge that have BPDU guard set to default shut down the interface on receiving a BPDU. In this case, the BPDU is not processed. You have two options. You can bring the interface up manually by using the NO SHUTDOWN command. Or, configure the errdisable-timeout feature with the SPANNING-TREE ERRDISABLE-TIMEOUT command to enable the interface after the specified time interval.

Use the SHOW SPANNING-TREE command to display the bridge and interface configurations for the BPDU guard feature. This command displays both the administratively configured and currently running values of BPDU guard.

Use the no form of the SPANNING-TREE BPDU-GUARD command to disable the BPDU-guard feature on a bridge.

Command Mode

Configuration Terminal mode

Example

The following commands enable the BPDU Guard feature on a bridge:

```
switch#configure terminal

switch(config)#spanning-tree portfast bpdu-guard
```

Related Commands

"SHOW SPANNING-TREE" on page 246

"SHUTDOWN" on page 187

"SPANNING-TREE ERRDISABLE-TIMEOUT" on page 252

SPANNING-TREE PORTFAST BPDU-GUARD ENABLE

Syntax

```
spanning-tree portfast bpdu-guard
enable|disable|default

no spanning-tree portfast bpdu-guard
```

Parameters

enable	Enables the BPDU-Guard feature on the switch. This configuration takes precedence over bridge configuration.
disable	Disables the BPDU-Guard feature on the switch. This configuration takes precedence over bridge configuration.
default	Indicates the bridge level BPDU-Guard configuration takes effect.

Description

The SPANNING-TREE PORTFAST BPDU-GUARD ENABLE command supersedes the bridge level configuration for the BPDU Guard feature. When the enable or disable parameter is used with this command, this configuration takes precedence over bridge configuration. However, when the default parameter is used with this command, the bridge-level-BPDU-guard configuration takes effect. Use the SPANNING-TREE PORTFAST BPDU-GUARD command to configure the BPDU Guard feature on a bridge.

Use the SHOW SPANNING-TREE command to display the bridge and interface configurations for the BPDU Guard feature. It shows both the administratively configured and currently running values of the BPDU-guard feature.

Command Mode

Configuration Terminal mode

Example

The following commands disable the BPDU guard feature on the switch:

```
switch#configure terminal

switch(config)#spanning-tree portfast bpdu-guard
disable
```

Related Commands

"SHOW SPANNING-TREE" on page 246

"SPANNING-TREE PORTFAST BPDU-GUARD" on page 262

SPANNING-TREE PRIORITY

Syntax

```
spanning-tree priority <0-61440>

no spanning-tree priority
```

Parameters

<0-61440>	Specifies the bridge priority value in increments of 4,096. For example, 4,096, 8,192, and 12,288 are all valid values.

Description

Use the SPANNING-TREE PRIORITY command to specify the interface priority. A lower priority value indicates a greater likelihood of becoming a root. The default value is 32,768.

The no form of this command resets the spanning-tree priority value to the default value which is 32,768.

Command Mode

Configuration Terminal mode

Example

The following commands set the spanning-tree priority on the switch:

```
switch#configure terminal

switch(config)#spanning-tree priority 4096
```

Related Commands

none

SPANNING-TREE RSTP ENABLE

Syntax

```
spanning-tree rstp enable

no spanning-tree rstp enable
```

Parameters

none

Description

Use the SPANNING-TREE RSTP ENABLE command to enable RSTP on the switch. After you have specified RSTP, all subsequent commands spanning tree commands apply to RSTP. Use the no form of this command to disable RSTP on the switch.

To make RSTP the active spanning tree mode and enable it on the switch, use the SPANNING TREE MODE command.

Command Mode

Configuration Terminal mode

Example

The following commands enable RSTP on the switch:

```
switch#configure terminal

switch(config)#spanning-tree rstp enable
```

Related Commands

"SPANNING-TREE MODE" on page 257

SPANNING-TREE STP ENABLE

Syntax

```
spanning-tree stp enable

no spanning-tree stp enable
```

Parameters

`enable` Specifies STP as the active spanning-tree protocol.

Description

Use the SPANNING-TREE STP ENABLE command to enable STP on the switch. After you have specified STP, all subsequent spanning tree commands apply to STP only. Use the no form of this command to disable STP on the switch.

To make STP the active spanning tree mode and enable it on the switch, use the SPANNING TREE MODE command.

Command Mode

Configuration Terminal mode

Example

The following commands enable STP on the switch:

```
switch#configure terminal

switch(config)#spanning-tree stp enable
```

Related Commands

“SPANNING-TREE MODE” on page 257

Chapter 14

Routing Information Protocol (RIP) Commands

The Routing Information Protocol (RIP) commands set the Layer 3 protocol.

This chapter contains the following commands:

CLEAR IP RIP ROUTE

Syntax

```
clear ip rip route A.B.C.D/M|all|connected|isis|
|kernel|ospf|rip|static
```

Parameters

A.B.C.D/M	Removes entries from the RIP routing table which match this destination address.
all	Clears the entire RIP routing table.
connected	Removes entries for connected routes from the RIP routing table.
isis	Removes only IS-IS routes from the RIP routing table
kernel	Removes kernel routes from the RIP routing table.
ospf	Removes only OSPF routes from the RIP routing table.
rip	Removes only RIP routes from the RIP routing table.
static	Removes static entries from the RIP routing table.

Description

Use the CLEAR IP RIP ROUTE command to clear data from the RIP routing table. To delete the RIP routes learned from a neighbor router and keep the RIP network intact, use the rip parameter with this command.

Using this command with the all parameter clears the RIP table of all the routes. If you do not want to delete a RIP network, use the REDISTRIBUTE CONNECTED command and make the RIP network a connected route.

Command Mode

View and Privileged Executive modes

Examples

The following command removes entries from the RIP routing table with the IP address of 10.0.0.0/8:

```
switch#clear ip rip route 10.0.0.0/8
```

The following command clears the entire RIP routing table:

```
switch#clear ip rip route rip
```

Related Commands

“REDISTRIBUTE CONNECTED” on page 295

DEFAULT-INFORMATION ORIGINATE

Syntax

```
default-information originate

no default-information originate
```

Parameters

none

Description

Use the DEFAULT-INFORMATION ORIGINATE command to distribute a default route to RIP. By default, this command is disabled. Use the no form of this command to disable this feature.

Command Mode

Router mode

Example

The following commands distribute a default route to RIP:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#default-information originate
```

Related Commands

none

DEFAULT-METRIC

Syntax

```
default-metric METRIC <1-16>

no default-metric METRIC
```

Parameters

METRIC	Indicates the default metric value. Choose a number between 1 and 16. By default, this command is set to 1.

Description

Use the DEFAULT-METRIC command to specify the metrics assigned to redistributed routes. This command is used with the REDISTRIBUTE CONNECTED command to make the routing protocol use the specified metric value for all redistributed routes. The DEFAULT-METRIC command is useful in redistributing routes with incompatible metrics. Every protocol has different metrics and cannot be compared directly. The default metric value provides the standard. All routes that are redistributed use the default metric value.

Use the no form of this command to disable this feature.

Command Mode

Router mode

Example

The following commands assign the cost of 10 to the OSPF routes which are redistributed into RIP:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#redistribute ospf

switch(config-router)#default-metric 10
```

Related Commands

“REDISTRIBUTE CONNECTED” on page 295

DISTANCE

Syntax

```
distance DISTANCE <1-255> A.B.C.D/M ACCESSLIST

no distance DISTANCE A.B.C.D/M ACCESSLIST
```

Parameters

DISTANCE	Specifies the administrative distance value. Choose a number between 1 and 255. By default, this parameter is set to 120.
A.B.C.D/M	Specifies an IP address and subnet mask in the following format: xxx.xxx.xxx\mask
ACCESSLIST	Specifies the access-list name. Use quotation marks to specify a list name with embedded spaces.

Description

Use the DISTANCE command to set the administrative distance. By default, the distance is set to 120.

Administrative distance is used by routers to select the path when there are two or more different routes to the same destination from two different routing protocols. A smaller administrative distance indicates a more reliable protocol.

Use the no form of this command to disable this function.

Command Mode

Router mode

Example

The following commands assign the administrative distance to 8, an IP address and subnet mask of 10.0.0.0/8, and an access list named "mylist":

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#distance 8 10.0.0.0/8 mylist
```

Reference

none

DISTRIBUTE-LIST

Syntax

```
distribute-list LIST in|out IFNAME

no distribute-list
```

Parameters

LIST	Specifies an access list. Choose from the following:
	in Filter incoming routing updates.
	out Filter outgoing routing updates.
IFNAME	Specifies a name of the interface.

Description

Use the DISTRIBUTE-LIST command to set the access list or the prefix list to filter incoming or outgoing route updates. By default, this command is disabled.

Filter out incoming or outgoing route updates using an access-list or a prefix list. If you do not specify the name of the interface, the filter is applied to all the interfaces.

Use the no form of this command to disable this feature.

Command Mode

Router mode

Example

The following commands filter incoming route updates using a prefix list called "myfilter" on interface 6:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#distribute-list myfilter in xe6
```

Related Commands

none

IP RIP AUTHENTICATION KEY-CHAIN

Syntax

```
ip rip authentication key-chain LINE

no ip rip authentication key-chain LINE
```

Parameters

LINE	Specifies the name of the authentication key chain. Enter an alphanumeric name. You do not have to use quotation marks to specify spaces.

Description

Use the IP RIP AUTHENTICATION KEY-CHAIN command to perform authentication on an interface and specify the name of the key chain. Not configuring the key chain results in no authentication. Use the no form of this command to disable this function.

Command Mode

Interface mode

Example

The following commands set the name of the key chain to “my key 1”on interface 6:

```
switch#configure terminal

switch(config)#interface xe6

switch(config-if)#ip rip authentication key-chain my
key 1
```

Related Commands

“KEY” on page 286, “KEY CHAIN” on page 287, “IP RIP AUTHENTICATION MODE” on page 279

IP RIP AUTHENTICATION MODE

Syntax

```
ip rip authentication mode md5|text

no ip rip authentication mode
```

Parameters

authentication mode	Specifies the type of authentication mode. Choose from the following options:	
	md5	Specifies the keyed MD5 authentication algorithm.
	text	Specifies clear text or simple password authentication.

Description

Use the IP RIP AUTHENTICATION MODE command to define the type of authentication mode used for RIP v2 packets received on the interface specified. By default, text authentication is enabled. Use the no form of this command to restore clear text authentication.

Command Mode

Interface mode

Example

The following commands set MD5 authentication on interface 1:

```
switch#configure terminal

switch(config)#interface xe1

switch(config-if)#ip rip authentication mode md5
```

Related Commands

"IP RIP AUTHENTICATION KEY-CHAIN" on page 278

IP RIP AUTHENTICATION STRING

Syntax

```
ip rip authentication STRING

no ip rip authentication STRING
```

Parameters

LINE	Specifies an authentication string or a password used by a key. Enter an alphanumeric value.

Description

Use the IP RIP AUTHENTICATION STRING command to define an authentication string or a password used by a key. Configure any receiving RIP packet on the interface with the same password.

The software provides the choice of configuring authentication for a single key or multiple keys at different times. Use this command to specify a password for a single key on an interface.

Command Mode

Interface mode

Example

The following commands set the authentication string to “Hahaha8” on interface 4:

```
switch#configure terminal

switch(config)#interface xe4

switch(config-if)#ip rip authentication “Hahaha8.”
```

Note
In the above example, configure any receiving RIP packet on interface 4 with the password “Hahaha8.”

Related Commands

none

IP RIP RECEIVE-PACKET

Syntax

```
ip rip receive-packet

no ip rip receive-packet
```

Parameters

none

Description

Use the IP RIP RECEIVE-PACKET command to enable an interface to receive RIP packets. By default, this command is enabled. Use the no form of this command to disable this feature.

Command Mode

Interface mode

Example

The following commands enable packets to be received on interface 2:

```
switch#configure terminal

switch(config)#interface xe2

switch(config-if)#ip rip receive-packet
```

Related Commands

"IP RIP SEND-PACKET" on page 283

IP RIP RECEIVE VERSION

Syntax

```
ip rip receive version 1|2

no ip rip receive version 1|2
```

Parameters

1 Specifies the acceptance of RIP version 1 packets.

2 Specifies the acceptance of RIP version 2 packets.

Description

Use the IP RIP RECEIVE-VERSION command to receive a specified version of RIP packets on an interface. This command overrides the setting of the VERSION command.

Use the no form of this command to use the setting specified with the VERSION command.

Command Mode

Interface mode

Example

The following command configures interface 5 to receive RIP version 1 packets:

```
switch#configure terminal

switch(config)#interface xe5

switch(config-if)#ip rip receive version 1
```

Related Commands

“VERSION” on page 308

IP RIP SEND-PACKET

Syntax

```
ip rip send-packet

no ip rip send-packet
```

Parameters

none

Description

Use the IP RIP SEND-PACKET command to enable an interface to send RIP packets. By default, this command is enabled. Use the no form of this command to disable this feature.

Command Mode

Interface mode

Example

The following command enables packets to be sent on interface 2:

```
switch#configure terminal

switch(config)#interface xe2

switch(config-if)#ip rip send-packet
```

Related Commands

none

IP RIP SEND VERSION

Syntax

```
ip rip send version 1|1-compatible|2

no ip rip send version 1|1-compatible|2
```

Parameters

1	Specifies the acceptance of RIP version 1 packets.
1-compatible	Specifies the acceptance of RIP version 1 compatible packets.
2	Specifies the acceptance of RIP version 2 packets.

Description

Use the IP RIP SEND-VERSION command to send a specified version of RIP packets on an interface. This command overrides the setting of the VERSION command.

Use the no form of this command to use the setting specified with the VERSION command.

Command Mode

Interface mode

Example

The following command enables RIP version 2 packets to be sent on interface 7:

```
switch#configure terminal

switch(config)#interface xe7

switch(config-if)#ip rip send version 2
```

Related Commands

“VERSION” on page 308

IP RIP SPLIT-HORIZON

Syntax

```
ip rip split-horizon poisoned

no ip rip split-horizon
```

Parameters

poisoned Specifies split-horizon with poisoned reverse.

Description

Use the IP RIP SPLIT-HORIZON command to perform the split-horizon action on the interface. The default is split-horizon poisoned.

Use this command to avoid including routes in updates sent to the same gateway from which they were learned. Using the IP RIP SPLIT-HORIZON command omits routes learned from one neighbor, in updates sent to that neighbor. Using the poisoned parameter with this command includes such routes in updates, but sets their metrics to infinity. Thus, advertising that these routes are not reachable.

Use the no form of this command to disable this function.

Command Mode

Interface mode

Example

The following command sets split-horizon to poisoned reverse on interface 7:

```
switch#configure terminal

switch(config)#interface xe7

switch(config-if)#ip rip split-horizon poisoned
```

Related Commands

none

KEY

Syntax

```
key <0-214783647>
```

Parameters

KEYID	Specifies the key identifier number. Choose a value between 0 and 214783647.

Description

Use the KEY command to manage, add, and delete authentication keys in a key chain.

Command Mode

Key Chain mode

Example

The following commands configure a key number of 199 and shows the prompt change:

```
switch#configure terminal

switch(config)#key chain mychain

switch(config-keychain)#key 199

switch(config-keychain-key)#
```

Related Commands

“IP RIP AUTHENTICATION KEY-CHAIN” on page 278

KEY CHAIN

Syntax

```
key CHAIN WORD
```

Parameters

WORD Specifies the key chain name.

Description

Use the KEY CHAIN command to access the Keychain mode. After you enter this mode, you can set a password for the key.

Command Mode

Configuration Terminal mode

Example

The following commands configure a key chain name of "k1" and shows the prompt change that indicates you have entered the Key Chain mode:

```
switch#configure terminal

switch(config)#key chain k1

switch(config-keychain)#
```

Related Commands

"IP RIP AUTHENTICATION KEY-CHAIN" on page 278, "KEY" on page 286

MAXIMUM-PREFIX

Syntax

```
maximum-prefix MAXPREFIX <1-65535> THRESHOLD <1-100>

no maximum-prefix MAXPREFIX <1-65535>
```

Parameters

MAXPREFIX	Indicates the maximum number of RIP routes allowed. Specify a value between 1 and 65,535.
THRESHOLD	Indicates the percentage of maximum routes that generate a warning. Specify a value between 1 to 100%. The default threshold is 75%. This is an optional parameter.

Description

Use the MAXIMUM-PREFIX command to configure the maximum prefix. If only one parameter is specified, the software interprets it as the MAXPREFIX value. Use the no form of this command to stop limiting the number of RIP routes in the routing table.

Command Mode

Router mode

Example

The following commands set the maximum prefix to 150 and the threshold to 80%:

```
switch#configure terminal

switch(config)# router rip

switch(config-router)#maximum-prefix 150 80
```

Related Commands

none

NEIGHBOR

Syntax

```
neighbor A.B.C.D

no neighbor A.B.C.D
```

Parameters

A.B.C.D	Specifies an IP address of a neighboring router with which the routing information is exchanged.

Description

Use the NEIGHBOR command to specify a neighbor router. This command is used for each connected point-to-point link. This command to exchange nonbroadcast routing information. It can be used multiple times for additional neighbors.

Use the no form of the command to disable a router. By default, the NEIGHBOR command is disabled.

The PASSIVE-INTERFACE command disables sending routing updates on an interface. Use the NEIGHBOR command in conjunction with the PASSIVE-INTERFACE command to send routing updates to specific neighbors.

Command Mode

Router mode

Example

The following commands create a neighbor with an IP address of 1.1.1.1:

```
Switch# configure terminal

Switch(config)# router rip

Switch(config-if)# neighbor 1.1.1.1
```

Related Commands

"PASSIVE-INTERFACE" on page 293

NETWORK

Syntax

```
network A.B.C.D|IFNAME

no network A.B.C.D|IFNAME
```

Parameters

A.B.C.D/M	Specifies the IP address prefix and subnet mask.
IFNAME	Specifies an interface name with an alphanumeric string.

Description

Use the NETWORK command to specify networks to which routing updates are sent to and received from. If a network is not specified, the interfaces in that network are not advertised in any RIP update. The default value is disabled.

Use the no form of this command to remove the specified network as one that runs RIP.

Command Mode

Router mode

Example

The following commands permit interface 1 to send to and receive RIP packets from network 10.0.0.0/8:

```
switch# configure terminal

switch(config)# router rip

switch(config-router)# network 10.0.0.0/8

switch(config-router)# network xe1
```

Related Commands

“CLEAR IP RIP ROUTE” on page 271, “SHOW IP RIP” on page 301

OFFSET-LIST

Syntax

```
offset-list ACCESSLIST in|out OFFSET <0-16> IFNAME
```

```
no offset-list
```

Parameters

ACCESSLIST	Specifies the access-list number or name.
in	Indicates the access list is used for metrics of incoming advertised routes.
out	Indicates the access list is used for metrics of outgoing advertised routes.
OFFSET	Specifies the offset that is used for metrics of networks matching the access list. Choose a value between 0 and 16. Setting the value to 0 indicates no change.
IFNAME	Specifies the interface name. For this command, specify "vlan1" only.

Description

Use the OFFSET-LIST command to specify the offset value that is added to the routing metric. When the networks match the access list, the offset value is applied to the metrics. By default, the OFFSET-LIST value is the interface metric which is defined by the operating system as 1.

Use the no form of this command to remove the offset list.

Command Mode

Router mode

Example

The following commands set the router to examine the RIP updates sent from VLAN 1 and adds 5 hops to the routes matching the IP addresses specified in access list 1:

```
switch#configure terminal
```

```
switch(config)#router rip
```

```
switch(config-router)#offset-list 1 in 5 vlan1
```

Related Commands

“ACCESS-LIST” on page 107

PASSIVE-INTERFACE

Syntax

```
passive-interface IFNAME

no passive-interface IFNAME
```

Parameters

IFNAME Specifies an interface name.

Description

Use the PASSIVE-INTERFACE command to block RIP broadcast on an interface. The default is disabled. Use the no form of this command to disable this function.

Command Mode

Router mode

Example

The following commands block RIP broadcasts on interface 2:

```
switch# configure terminal

switch(config)# router rip

switch(config-router)# passive-interface xe2
```

Related Commands

"SHOW IP RIP" on page 301

RECV-BUFFER-SIZE

Syntax

```
recv-buffer-size <8192-2147483647>

no recv-buffer-size
```

Parameters

<8192-2147483647>	Specifies the RIP UDP receive buffer size value.

Description

Use the RECV-BUFFER-SIZE command to run-time configure the RIP UDP receive-buffer size. The system default value is 8,192. Use the no form of this command to remove the configured RIP UDP receive-buffer size and return it to the default value.

Command Mode

Router mode

Example

The following commands set the RIP UDP receive-buffer size to 23,456,789:

```
switch# configure terminal

switch(config)# router rip

switch(config)# recv-buffer-size 23456789
```

Related Commands

none

REDISTRIBUTE CONNECTED

Syntax

```
redistribute connected|isis|kernel|ospf|static| METRIC
<0-16> ROUTEMAP

no redistribute connected|isis|kernel|ospf|static|
METRIC <0-16> ROUTEMAP
```

Parameters

connected	Specifies redistribute information from connected routes.
isis	Specifies redistribute information from IS-IS.
kernel	Specifies redistribute information from kernel routes.
ospf	Specifies redistribute information from OSFP.
static	Specifies redistribute information from static routes.
METRIC	Specifies a metric value to be used in redistributing information. Choose a value between 0 and 16.
ROUTEMAP	Specifies a route map that is used to redistribute information. Choose an alphanumeric name that is a pointer to route-map entries.

Description

Use the REDISTRIBUTE CONNECTED command to redistribute information from other routing protocols. Use the no form of this command to disable this function.

Command Mode

Router mode

Example

Use the following commands to redistribute information from kernel routes using a metric of 8 and a route-map called "IPI":

```
switch# configure terminal

switch(config)# router rip

switch(config-router)# redistribute connected kernel
metric 8 route-map ipi
```

Related Commands

none

ROUTE

Syntax

```
route A.B.C.D/M

no route A.B.C.D/M
```

Parameters

A.B.C.D/M Specifies the IP address prefix and length.

Description

Use the ROUTE command to add a static RIP route. This command is most commonly used for debugging purposes and is not displayed in the kernel routing table. After adding the RIP route, you can check the route in the RIP routing table.

Use the no form of this command to disable this function.

Command Mode

Router mode

Example

The following commands configure static RIP route with an IP address and a mask of 10.10.10.11/8.

```
switch# configure terminal

switch(config)# router rip

switch(config-router)# route 10.10.10.11/8
```

Related Commands

"CLEAR IP RIP ROUTE" on page 271, "SHOW IP RIP" on page 301

ROUTER RIP

Syntax

```
router rip

no router rip
```

Parameters

none

Description

Use the ROUTER RIP command to enable a RIP routing process on the switch and enter the Router command mode. After you enter this command, the prompt changes to indicate the new mode. Use the no form of this command to disable the RIP routing process.

Command Mode

Configuration Terminal mode

Examples

The following commands sets the command mode to the router mode:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#
```

The following commands begin the RIP routing process:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#version 1

switch(config-router)#network 10.10.10.0/24

switch(config-router)#network 10.10.11.0/24

switch(config-router)#neighbor 10.10.10.10
```

Related Commands

"NETWORK" on page 290, "VERSION" on page 308

SHOW IP PROTOCOLS RIP

Syntax

```
show ip protocols rip
```

Parameters

none

Description

Use the SHOW IP PROTOCOLS RIP command to display RIP process parameters and statistics. To modify the lines displayed, use “|” the output modifier token. To save the output to a file, use “>,” the output redirection token.

Command Mode

View and Privileged Executive modes

Example

The following command displays RIP process parameters and statistics:

```
switch#show ip protocols rip

Routing Protocol is “rip”
Sending updates every 30 seconds with +/-50%, next due in 12
seconds
Timeout after 180 seconds, garbage collect after 120 seconds
Outgoing update filter list for all interfaces is not set
Incoming update filter list for all interfaces is not set
Default redistribution metric is 1
Redistributing: connected static
Default version control: send version 2, receive version 2
Interface Send Recv Key-chain
xe1               2           2

Routing for Networks:
  10.10.0.0/24
Routing Information Sources:
Gateway    Distance  Last Update   BadPackets   BadRoutes
Distance: default is 120
```

Related Commands

none

SHOW IP RIP

Syntax

```
show ip rip
```

Parameters

none

Description

Use the SHOW IP RIP command to display RIP routes. To modify the lines displayed, use "|" the output modifier token. To save the output to a file, use ">," the output redirection token.

Command Mode

View and Privileged Executive modes

Example

The following command displays the RIP routing table with the destination network, nexthop, and metric to reach it:

```
switch#show ip rip

Codes: R - RIP, Rc - RIP connected, RS - RIP static,
K - Kernel, C - Connected, S - Static, O - OSPF,
I - IS-IS, B - BGP
```

Network	Next Hop	Metric	From	If	Time
Rc 10.10.10.0/24		1		vlan1	
R 10.10.11.0/24	10.10.10.38	2	10.10.10.33	vlan1	02:42

See the Table 16 for the definitions of the previous example.

Table 16. SHOW IP RIP

Heading	Definition
Network	Specifies the routing code (see list above) as well as the IP address and subnet mask of the network.
Next Hop	Specifies the IP address of the next hop.
Metric	Indicates the number of hops.

Table 16. SHOW IP RIP (Continued)

Heading	Definition
From	Indicates the IP address where the route is learned from.
If	Indicates the name of the interface.
Time	Indicates the length of time when the route was learned. This value is in minutes and seconds.

Related Commands

“ROUTE” on page 297, “NETWORK” on page 290, “CLEAR IP” on page 47

Equivalent Command

“SHOW IP RIP DATABASE” on page 303

SHOW IP RIP DATABASE

Syntax

```
show ip rip database
```

Parameters

none

Description

Use the SHOW IP RIP DATABASE command to display information about the RIP database. To modify the lines displayed, use "|" the output modifier token. To save the output to a file, use ">," the output redirection token.

Command Mode

View and Privileged Executive modes

Example

The following command displays the RIP database information.

```
switch#show ip rip database

Codes: R - RIP, K - Kernel, C - Connected, S - Static, O -
OSPF, I - IS-IS, B - BGP

   Network   Next Hop          Metric From    If   Time
   K        0.0.0.0/0          10.0.1.1 16   xe2  01:58
   C        10.0.1.0/24 1                    xe2
   S        10.10.10.0/24 1                  xe2
   C        10.10.11.0/24 1                  xe2
   S        192.168.101.0/24  1              xe2
   R        192.192.192.0/24  1              --
```

See Table 16 on page 301 for a definition of the command headings.

Related Commands

"ROUTE" on page 297, "NETWORK" on page 290, "CLEAR IP" on page 47

Equivalent Command

"SHOW IP RIP" on page 301

SHOW IP RIP INTERFACE

Syntax

```
show ip rip interface IFNAME
```

Parameters

IFNAME	Specifies the interface name. This is an optional parameter. If you do not specify an interface to display, information about all of the interfaces is displayed.

Description

Use the SHOW IP RIP INTERFACE command to display information about the RIP interfaces. You can specify an interface name to display information about a specific interface.

To modify the lines displayed, use “|” the output modifier token. To save the output to a file, use “>,” the output redirection token.

Command Mode

View and Privileged Executive modes

Example

The following command displays the RIP interface information for all of the interfaces:

```
switch#show ip rip interface

eth0 is down, line protocol is down
   RIP is not enabled on this interface
eth1 is down, line protocol is down
   RIP is not enabled on this interface
lo is down, line protocol is down
   RIP is not enabled on this interface
vlan1 is down, line protocol is down
   RIP is not enabled on this interface
xe1 is up, line protocol is up
   RIP is enabled on this interface
xe2 is up, line protocol is up
   RIP is enabled on this interface
xe3 is up, line protocol is up
   RIP is enabled on this interface
xe4 is up, line protocol is up
   RIP is enabled on this interface
xe5 is down, line protocol is down
   RIP is not enabled on this interface
```

```
xe6 is down, line protocol is down
   RIP is not enabled on this interface
xe7 is down, line protocol is down
   RIP is not enabled on this interface
xe8 is down, line protocol is down
   RIP is not enabled on this interface
```

Related Commands

none

TIMERS BASIC

Syntax

```
timers basic UPDATE <5-2147483647>
TIMEOUT <5-2147483647> GARBAGE <5-2147483647>

no timers basic
```

Parameters

UPDATE	Specifies the routing table update timer in seconds. The default value is 30 seconds. Choose a value between 5 and 2,147,483,647.
TIMEOUT	Specifies the routing information timeout timer in seconds. The default value is 180 seconds. After this interval has elapsed and no updates for a route are received by the software, the route is declared invalid. However, it is not removed from the routing table. Choose a value between 5 and 2,147,483,647.
GARBAGE	Specifies the routing garbage collection timer in seconds. The default value is 120 seconds. After this interval has elapsed, the route is removed from the routing table. Choose a value between 5 and 2,147,483,647.

Description

Use the TIMERS BASIC command to adjust basic routing protocol update timers. This command adjusts the RIP timing parameters. Every 30 seconds, the AT-S83 software sends an update that contains the complete routing table to every neighboring router. When the time specified by the TIMEOUT parameter expires, the route is no longer valid. However, a route is retained in the routing table for a short time so that neighboring routers are notified that the route has been dropped. When the time specified by the GARBAGE parameter expires, the route is removed from the routing table.

Note
The route is included in all updates sent by the router until the time specified by the GARBAGE parameter expires.

All routers in the network must have the same timers defined to allow RIP to execute a distributed and asynchronous routing algorithm. The timers should not be synchronized as this may lead to unnecessary collisions on the network.

Use the no form of the TIMERS BASIC command to restore the default values to the timers.

Command Mode

Router mode

Example

The following commands set the UPDATE timer to 30 seconds, TIMEOUT timer to 180 seconds, and the GARBAGE timer 120 seconds:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)#timers basic 30 180 120
```

Related Commands

none

VERSION

Syntax

```
version 1|2

no version
```

Parameters

1 Specifies version 1 of the RIP.

2 Specifies version 2 of the RIP. This is the default.

Description

Use the VERSION command to enable a RIP routing process globally on the switch. After you enter this command, the prompt changes.

RIP can run in version 1 or version 2 modes. Version 2 includes authentication and is more feature rich than version 1. One you set the RIP version, RIP packets of the specified version are received and sent on all of the RIP-enabled interfaces on the switch.

Use the no form of this command to restore version 2 of RIP.

Note
The IP RIP RECEIVE VERSION command and the IP RIP SEND VERSION command override the value set by the VERSION command.

Command Mode

Router mode

Example

The following commands enable RIP version 1 on the switch:

```
switch#configure terminal

switch(config)#router rip

switch(config-router)# version 1
```

Related Commands

"IP RIP RECEIVE VERSION" on page 282, "IP RIP SEND VERSION" on page 284

Chapter 15

Open Shortest Path First (OSPF) Commands

This chapter contains the following commands:

AUTO-COST REFERENCE-BANDWIDTH

Syntax

auto-cost reference-bandwidth <1-4294967>

no auto-cost reference-bandwidth

Parameters

reference-bandwidth	Specifies the reference bandwidth in Mbits per second.

Description

Use the AUTO-COST REFERENCE-BANDWIDTH command to control how OSPF calculates default metrics for the interface. The reference bandwidth is measured by Mbits per second. The default value for the reference bandwidth is 100Mbps.

By default, OSPF calculates the OSPF metric for an interface by dividing the reference bandwidth by the interface bandwidth. This command is used to differentiate high bandwidth links. For multiple links with high bandwidth, specify a larger reference bandwidth value to differentiate cost on those links.

Use the no form of this command to assign cost, based only on the interface bandwidth.

Command Mode

Router mode

Example

The following commands set the reference bandwidth to 50 Mbits per second:

```
switch#configure terminal

switch(config)#router ospf 100

switch (config-router)# auto-cost reference-bandwidth
50
```

Related Commands

“IP OSPF COST” on page 319

COMPATIBLE RFC1583

Syntax

compatible rfc1583

no compatible rfc1583

Parameters

none

Description

Use the COMPATIBLE RFC1583 command to restore the method used to calculate summary route costs per RFC. By default, OSFP is compatible with RFC 2328.

Prior to RFC 2328, OSPF was compliant with RFC 1583 which specified the method for calculating the metric for summary routes based on the minimum metric of the component paths available. RFC 2328 specifies a method for calculating metrics based on the maximum cost. With this change, it is possible that all of the ABRs in an area might not be upgraded to the new code at the same time. The COMPATIBLE RFC1583 command addresses this issue and allows the selective disabling of compatibility with RFC 2328.

Use the no form of this command with the COMPATIBLE RFC1583 command to disable RFC 1583 compatibility.

Command Mode

Router mode

Example

The following commands set OSPF compatible to RFC 1583:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)# compatible rfc1583
```

Related Commands

none

HOST AREA

Syntax

```
host A.B.C.D area AREAID (COST)

no host A.B.C.D area AREAID (COST)
```

Parameters

A.B.C.D	Specifies the IP address of the host.	
AREAID	Specifies an area id. Choose from the following:	
	A.B.C.D	Specifies an OSPF area ID in IPv4 address format.
	0 to 4,294,967,295	Specifies an Area ID as 4 octets unsigned integer value.
INTERFACENAME	Specifies the name of the interface.	
COST	Specifies the cost for stub host entry. Enter a value between 0 to 65,535. This is an optional parameter.	

Description

Use the HOST AREA command to configure a stub host entry belonging to a particular area. This command permits you to advertise specific host routes in the router-LSA as a stub link. You can perform the same task with the HOST AREA command.

Since the stub host belongs to the specified router, specifying cost is not important. By default, no host entry is configured.

Use the no form of this command to remove the host area configuration.

Command Mode

Router mode

Example

The following commands set area 1 to an IP address of 172.16.10.100 and area 2 to an IP address of 172.16.10.101 with a cost of 10:

```
switch#configure terminal

switch(config)#router ospf 100
```

```
switch(config-router)# host 172.16.10.100 area 1

switch(config-router)# host 172.16.10.101 area 2 cost
10
```

Related Commands

"NETWORK AREA" on page 340

IP OSPF AUTHENTICATION

Syntax

```
ip ospf (A.B.C.D) authentication (message-digest|null)

no ip ospf (A.B.C.D) authentication
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
message-digest	Specifies the message digest authentication.
null	Specifies no authentication. This parameter overrides password or message-digest authentication of the interface.

Description

Use the IP OSPF AUTHENTICATION command to send and receive OSPF packets with the specified authentication method. This command enables OSPF packets to use authentication on the current interface.

Use the no form of this command to disable the authentication.

Command Mode

Interface mode

Example

In this example, interface 2 is set to have no authentication. This configuration overrides any text or MD5 authentication configured on this interface:

```
switch#configure terminal

switch(config)#interface xe1

switch(config-if)# ip ospf authentication null
```

Related Commands

“IP OSPF AUTHENTICATION-KEY” on page 317,“IP OSPF MESSAGE-DIGEST-KEY” on page 326

IP OSPF AUTHENTICATION-KEY

Syntax

```
ip ospf (A.B.C.D) authentication-key LINE

no ip ospf (A.B.C.D) authentication-key
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
LINE	Specifies the authentication password. String by the end of the line is taken.

Description

Use the IP OSPF AUTHENTICATION-KEY command to specify an OSPF authentication password for the neighboring routers. This command creates a password (key) that is inserted into the OSPF header when the software originates routing protocol packets. Assign a separate password to each network for different interfaces. All neighboring routers on the same network with the same password exchange OSPF routing data.

The key can be used only when authentication is enabled for an area. Use the AREA AUTHENTICATION command to enable authentication.

Simple password authentication allows you to configure a password for each area. Configure the routers in the same routing domain with the same password.

Use the no form of this command to remove an OSPF authentication password. By default, the authentication password is not specified.

Command Mode

Interface mode

Example

In the following example, an authentication key test is created on interface 3 in area 0. Note that first authentication is enabled for area 0:

```
switch# configure terminal

switch(config)# router ospf 100

switch(config-router)# network 10.10.10.0/24 area 0
```

```
switch(config-router)# area 0 authentication

switch(config-router)# exit

switch(config)# interface xe3

switch(config-if)# ip ospf 193.43.23.3 authentication-
key test
```

Related Commands

“IP OSPF AUTHENTICATION” on page 316

IP OSPF COST

Syntax

```
ip ospf (A.B.C.D) cost COST <1-65535>

no ip ospf (A.B.C.D) cost
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
COST	Specifies the link-state metric. The default value is 10. Enter a value between 1 to 65,535.

Description

Use the IP OSPF COST command to specify the cost of link-state metric in a router-LSA. The interface cost indicates the overhead required to send packets across the interface specified. This cost is stated in the Router-LSA's link. The cost is inversely proportional to the bandwidth of an interface. By default, the cost of an interface is calculated based on the bandwidth (10^8/ bandwidth). Use the IP OSPF COST command to set the cost manually.

Use the no form of this command to reset the interface cost to the default value.

Command Mode

Interface mode

Example

The following example sets the OSPF cost value to 12 on interface 3 for IP address 192.43.23.23:

```
switch# configure terminal

switch(config)# interface xe3

switch(config-if)# ip ospf 192.43.23.23 cost 12
```

Related Commands

"AUTO-COST REFERENCE-BANDWIDTH" on page 312

IP OSPF DATABASE-FILTER

Syntax

```
ip ospf (A.B.C.D) database-filter all out

no ip ospf (A.B.C.D) database-filter
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
all	Specifies all LSAs are filtered.
out	Specifies outgoing LSAs are filtered.

Description

Use the IP OSPF DATABASE-FILTER command to turn on the LSA database-filter for a particular interface. By default, this command is disabled which means that all outgoing LSAs are flooded to the interface.

OSPF floods new LSAs over all interfaces in an area, except the interface on which the LSA arrives. This redundancy ensures robust flooding. However, too much redundancy can waste bandwidth and might lead to excessive link and CPU usage in certain topologies, resulting in destabilizing the network. To avoid this issue, use the IP OSPF DATABASE-FILTER command to block flooding of LSAs over specified interfaces.

Use the no form of this command to turn off the filter.

Command Mode

Interface mode

Example

The following example filters all LSAs and outgoing LSAs on interface 3:

```
switch# configure terminal

switch(config)# interface xe3

switch(config-if)# ip ospf database-filter all out
```

Related Commands

none

IP OSPF DEAD-INTERVAL

Syntax

```
ip ospf (A.B.C.D) dead-interval INTERVAL <1-65535>

no ip ospf (A.B.C.D) dead-interval
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
INTERVAL	Specifies the interval in seconds. Choose a value between 1 and 65,535. The default interval is 40 seconds.

Description

Use the IP OSPF DEAD-INTERVAL command to set the interval during which no hello packets are received and after which a neighbor is declared dead.

The dead-interval is the amount of time that the router waits to receive an OSPF hello packet from the neighbor before declaring the neighbor down. This value is advertised in the router's hello packets. It must be a multiple of the hello-interval and be the same for all routers on a specific network.

Use the no form of this command to return to the default time. If you have configured this command specifying the IP address of the interface and want to remove the configuration, use the no form of this command with the specified IP address.

Command Mode

Interface mode

Example

The following example shows configuring dead-interval for 10 seconds on interface 2:

```
switch# configure terminal

switch(config)# interface xe2

switch(config-if)# ip ospf dead-interval 10
```

Related Commands

"IP OSPF HELLO-INTERVAL" on page 325

IP OSPF DISABLE ALL

Syntax

```
ip ospf (A.B.C.D) disable all
```

Parameters

all Specifies all OSPF functionality.

Description

Use the IP OSPF DISABLE ALL command to completely disable OSPF packet processing on an interface.

This command overrides the NETWORK AREA command and disables the processing of packets on the interface specified. For more information about this command, see “NETWORK AREA” on page 340.

Command Mode

Interface mode

Example

The following example shows disables OSPF on interface 2:

```
switch# configure terminal

switch(config)# interface xe2

switch(config-if)# ip ospf disable all
```

Related Commands

“NETWORK AREA” on page 340

IP OSPF HELLO-INTERVAL

Syntax

```
ip ospf (A.B.C.D) hello-interval INTERVAL <1-65535>

no ip ospf (A.B.C.D) hello-interval
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
INTERVAL	Specifies the interval in seconds. Choose a value between 1 and 65,535. The default interval is 10 seconds.

Description

Use the IP OSPF HELLO-INTERVAL command to specify the interval between hello packets.

The hello-interval is advertised in the hello packets. Configure the same hello-interval for all routers on a specific network. A shorter hello interval ensures faster detection of topological changes, but results in more routing traffic.

Use the no form of this command to return to it to the default value.

Command Mode

Interface mode

Example

The following example shows setting the hello-interval for 3 seconds on interface 3:

```
switch# configure terminal

switch(config)# interface xe3

switch(config-if)# ip ospf hello-interval 3
```

Related Commands

"IP OSPF DEAD-INTERVAL" on page 322

IP OSPF MESSAGE-DIGEST-KEY

Syntax

```
ip ospf A.B.C.D message-digest-key KEYID <1-255> md5
LINE

no ip ospf A.B.C.D message-digest-key KEYID
```

Parameters

A.B.C.D	Specifies the IP address of the interface.
KEYID	Specifies a key ID. Enter a value between 1 and 255.
MD5	Specifies the MD5 algorithm.
LINE	Specifies the OSPF password. String by the end of the line is taken. Enter a value between 1 and 16 characters.

Description

Use the IP OSPF MESSAGE-DIGEST-KEY command to register an MD5 key for OSPF MD5 authentication. By default, this command is disabled.

Message Digest Authentication is a cryptographic authentication. A key (password) and key-id are configured on each router. The router uses an algorithm based on the OSPF packet, the key, and the key-id to generate a message digest that is appended to the packet.

Use this command for uninterrupted transitions between passwords. This is helpful for administrators who want to change the OSPF password without disrupting communication. The system begins a rollover process until all the neighbors have adopted the new password. This allows neighboring routers to continue communication while the network administrator is updating them with a new password. The router stops sending duplicate packets once it detects that all of its neighbors have adopted the new password.

Maintain only one password per interface, removing the old password when you add a new one. This prevents the local system from continuing to communicate with the system that is using the old password. Removing the old password also reduces overhead during rollover.

All neighboring routers on the same network must have the same password value to enable exchange of OSPF routing data.

Use the no form of the IP OSPF MESSAGE-DIGEST-KEY command to remove an MD5 key.

Command Mode

Interface mode

Examples

The following example shows OSPF authentication on interface 2, key password of "1,", MD5 authentication, and an OSPF password of "april12pass:"

```
switch# configure terminal
switch(config)# interface xe2
switch(config-if)# ip ospf authentication message-
digest
switch(config-if)# ip ospf message-digest-key 1 md5
april12pass
```

The following example shows OSPF authentication on interface 1 with an IP address of 1.1.1.1, a key of "2," MD5 authentication, and an OSPF password of "yourpass45:"

```
switch# configure terminal

switch(config)# interface xe1

switch(config-if)# ip ospf 1.1.1.1 authentication
message-digest

switch(config-if)# ip ospf 1.1.1.1 message-digest-key
2 md5 yourpass45
```

Note
If an interface has two IP addresses assigned-- 198.89.9.1 & 198.89.9.2, OSPF authentication is enabled only for the first IP address (198.89.9.1).

Related Commands

none

IP OSPF MTU

Syntax

```
ip ospf (A.B.C.D) mtu <576-65535>

no ip ospf (A.B.C.D) mtu <576-65535>
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
<576-65535>	Specifies the MTU size. Choose a value between 576 and 65535.

Description

Use the IP OSPF MTU command to set the MTU size for OSPF to construct packets based on this value. By default, OSPF uses the interface MTU derived from the kernel.

When OSPF constructs packets, it uses interface the MTU size as maximum IP packet size. This command forces OSPF to use the specified value, overriding the actual interface MTU size.

This command allows an administrator to configure the MTU size the recognized by the OSPF protocol. It does not configure the MTU settings on the kernel. OSPF will not recognize MTU size configuration changes made to the kernel until the MTU size is updated through the CLI.

Use the no form of this command to return the command to its default value.

Command Mode

Interface mode

Example

The following commands set the MTU size to 1480 on interface 4:

```
switch# configure terminal

switch(config)# interface xe4

switch(config-if)# ip ospf mtu 1480
```

Related Commands

none

IP OSPF MTU-IGNORE

Syntax

```
ip ospf (A.B.C.D) mtu-ignore

no ip ospf (A.B.C.D) mtu-ignore
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.

Description

Use the IP OSPF MTU-IGNORE command to configure OSPF so that it does not check the MTU size during DD (Database Description) exchange.

By default, OSPF checks the MTU size described in DD packets received from the neighbor during the DD exchange process. If the MTU size does not match the interface MTU, neighbor adjacency is not established. Using this command makes OSPF ignore this check and allows adjacency to be established regardless of MTU size in the DD packet.

Use the no form of this command to make sure that OSPF checks MTU size during DD exchange.

Command Mode

Interface mode

Example

The following example sets the OSPF so that it does not check the MTU size during DD exchange on interface 4:

```
switch# configure terminal

switch(config)# interface xe4

switch(config-if)# ip ospf mtu-ignore
```

Related Commands

none

IP OSPF NETWORK

Syntax

```
ip ospf network broadcast|non-broadcast|point-to-
point|point-to-multipoint

no ip ospf network
```

Parameters

broadcast	Sets the network type to broadcast.
non-broadcast	Sets the network type to Nonbroadcast Multiple Access network (NBMA).
point-to-multipoint	Sets the network type to point-to-multipoint.
point-to-point	Sets the network type to point-to-point.

Description

Use the IP OSPF NETWORK command to force the interface network type to the type specified. Depending on the network type, OSPF changes the behavior of the sending packet and describes link in LSAs.

Use the no form of this command to return it to the default value. The default value is Broadcast type.

Command Mode

Interface mode

Example

The following example sets the network to point-to-point type on the interface 1:

```
switch#configure terminal

switch(config)#interface xe1

switch(config-if)# ip ospf network point-to-point
```

Related Commands

none

IP OSPF PRIORITY

Syntax

```
ip ospf (A.B.C.D) priority PRIORITY <0-255>

no ip ospf (A.B.C.D) priority
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
PRIORITY	Specifies the router priority of the interface. Choose a value between 0 and 255. The default value is 1.

Description

Use the IP OSPF NETWORK command to set the router priority to determine the OSPF Designated Router (DR) for a network. When configuring this command, use the following guidelines:

- If two routers attempt to become the DR, the router with the higher router priority becomes the DR.
- If the router priority is the same for two routers, the router with the higher router ID takes precedence.
- Only routers with nonzero router priority values are eligible to become the designated or backup-designated router.
- Configure the router priority for multiaccess networks only and not for point-to-point networks.

Use the no form of this command to return it to the default value. The default priority is 1.

Command Mode

Interface mode

Example

The following example shows setting the OSPF priority value to 3 on interface 2:

```
switch# configure terminal

switch(config)# interface xe2

switch(config-if)# ip ospf priority 3
```

Related Commands

"IP OSPF NETWORK" on page 331

IP OSPF RETRANSMIT-INTERVAL

Syntax

```
ip ospf retransmit-interval INTERVAL <1-65535>

no ip ospf retransmit-interval
```

Parameters

INTERVAL	Specifies the interval in seconds. Choose a value between 1 and 65535 seconds. The default interval is 5 seconds.

Description

Use the IP OSPF RETRANSMIT-INTERVAL command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface.

After sending an LSA to a neighbor, the router keeps the LSA until it receives an acknowledgement. In case the router does not receive an acknowledgement during the set time (the retransmit interval value), it retransmits the LSA. Set the retransmission interval value conservatively to avoid needless retransmission. The interval should be greater than the expected round-trip delay between two routers.

Use the no form of this command to return it to the default value. The default interval is 5 seconds.

Command Mode

Interface mode

Example

The following example sets the OSPF retransmit interval to 6 seconds on interface 4:

```
switch# configure terminal

switch(config)# interface xe4

switch(config-if)# ip ospf retransmit-interval 6
```

Related Commands

none

IP OSPF TRANSMIT-DELAY

Syntax

```
ip ospf (A.B.C.D) transmit-delay DELAY <1-65535>

no ip ospf (A.B.C.D) transmit-delay
```

Parameters

A.B.C.D	Specifies the IP address of the interface. This is an optional parameter.
DELAY	Specifies the time interval, in seconds, to transmit a link-state update. Choose a value between 1 and 65,535 seconds. The default interval is 1 second.

Description

Use the IP OSPF TRANSMIT-DELAY command to specify the time between link-state advertisement (LSA) retransmissions for adjacencies belonging to the interface. The default interval is 1 second.

The transmit delay value adds a specified time to the age field of an update. If the delay is not added, the time in which the LSA transmits over the link is not considered. This command is especially useful for low speed links. Add transmission and propagation delays when setting the transmit delay value.

Use the no form of this command to return it to the default value.

Command Mode

Interface mode

Example

The following example sets the OSPF transmit delay time to 6 seconds on interface 4.

```
switch# configure terminal

switch(config)# interface xe4

switch(config-if)# ip ospf transmit-interval 6
```

Related Commands

none

MAX-CONCURRENT-DD

Syntax

```
max-concurrent-dd <1 - 65535>
```

Parameters

none

Description

Use the MAX-CONCURRENT-DD command to set the limit for the number of Database Descriptors (DD) processes that can be processed concurrently. Use this command to set the limit for the number of DDs that can be processed concurrently. Specify a value between 1 and 65,535.

This command is useful when a router's performance is affected from simultaneously bringing up several OSPF adjacencies. The MAX-CONCURRENT-DD command limits the maximum number of DD exchanges that can occur concurrently per OSPF instance, thus allowing for all of the adjacencies to come up.

Command Mode

Router mode

Example

The following commands set the processing of 4 DD processes at a time:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)#max-concurrent-dd 4
```

Related Commands

none

MAX-UNUSE-PACKET

Syntax

max-unuse-packet <0 - 65535>

no max-unuse-packet

Parameters

none

Description

Use the MAX-UNUSE-PACKET command to set the maximum number of unused OSPF packets maintained internally to avoid additional memory allocation and deletion. Specify a value between 0 and 65,535.

Use the no form of this command to return it to the default value. The default value is 200.

Command Mode

Router mode

Example

The following example sets the MAX-UNUSE-PACKET value to a maximum of 300 unused OSPF packets:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)#max-unuse-packet 300
```

Related Commands

none

NEIGHBOR

Syntax

```
neighbor A.B.C.D (COST <1-65535>) POLL-
INTERVAL|PRIORITY

no neighbor A.B.C.D (COST <1-65535>) POLL-
INTERVAL|PRIORITY
```

Parameters

A.B.C.D	Specifies an IP address of a neighboring router.
COST	Specifies the link-state metric to this neighbor. Enter a value between 1 and 65,535. This is an optional parameter.
POLL-INTERVAL	Specifies the dead neighbor polling interval in seconds. Enter a value between 1 and 65,535. Allied Telesis recommends setting this value much higher than the hello interval. The default value is 120 seconds.
PRIORITY	Specifies the 8-bit number indicating the router priority value of the non-broadcast neighbor associated with the specified IP address. Enter a value between 0 and 255. This keyword does not apply to point-to-multipoint interfaces. The default value is 0.

Description

Use the NEIGHBOR command to configure OSPF routers interconnecting to NMBA networks.

To configure a neighbor on an NBMA network manually, use the NEIGHBOR command and include one neighbor entry for each known nonbroadcast network neighbor. Configure the neighbor address on the primary address of the interface.

The poll interval is the reduced rate at which routers continue to send hello packets when a neighboring router has become inactive. Set the poll interval to be much larger than hello interval.

Use the no form of the command to remove a configuration.

Command Mode

Router mode

Example

This example shows the NEIGHBOR command configured with a priority value of 1:

```
switch# configure terminal

switch(config)# router rip

switch(config-if)# neighbor 1.2.3.4 priority 1
```

Related Commands

none

NETWORK AREA

Syntax

```
network A.B.C.D/M|A.B.C.D X.Y.Z.W area A.B.C.D|<0-4294967295>

no network A.B.C.D/M|A.B.C.D X.Y.Z.W area A.B.C.D|<0-4294967295>
```

Parameters

A.B.C.D/M	Indicates a IPv4 network address followed by a subnet mask address (in prefix length format).
A.B.C.D X.Y.Z.W	Specifies an IPv4 network address followed by a wildcard mask.
A.B.C.D	Specifies an OSPF Area ID in IPv4 address format.
<0-4294967295>	Specifies an OSPF Area ID as 4 octets unsigned integer value.

Description

Use the NETWORK AREA command to enable OSPF routing with a specified Area ID on interfaces with IP addresses that match the specified network address. You can assign one area to multiple network addresses. By default, no network area is configured. You can perform the same task with the HOST AREA command.

OSPF routing can be enabled per IPv4 subnet basis. Each subnet can belong to one particular OSPF area. A network address can be defined using the prefix length or a wild card mask. A wild card mask is comprised of consecutive 0’s as network bits and consecutive 1’s as host bits.

There are two ways to define the subnet mask. You can define the subnet mask in the traditional way or you can use the prefix length format as an abbreviated method of defining a subnet mask. SeeTable 17.

Table 17. Prefix Length Format

Prefix Length Format	Subnet Mask
/8	255.0.0.0
/16	255.255.0.0
/24	255.255.255.0

Use the no form of this command to disassociate a network address from an area. In addition, you can use the no form of this command to remove the host area configuration.

Command Mode

Router mode

Examples

The following commands set the network address of 10.0.0.0/8 to an area id of 3:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)# network 10.0.0.0/8 area 3
```

The following commands set the network address of 192.168.0.0 and a subnet mask of 255.255.0.0 to an area id of 12:

```
switch#configure terminal

switch(config)#router ospf 90

switch(config-router)# network 192.168.0.0 255.255.0.0
area 12
```

Related Commands

"HOST AREA" on page 314

OSPF ABR-TYPE

Syntax

```
ospf abr-type cisco|ibm|shortcut|standard

no ospf abr-type cisco|ibm
```

Parameters

cisco	Specifies an alternative OSPF Area Border Router (ABR) type using Cisco implementation RFC 3509. This is the default ABR type.
ibm	Specifies an alternative ABR using IBM implementation RFC 3509.
shortcut	Specifies a Shortcut ABR as defined by draft-jetf-ospf-shortcut-abr-02.txt.
standard	Specifies a standard behavior ABR as defined by RFC 2328.

Description

Use the OSPF ABR-TYPE command to set an ABR type. Specifying the ABR type allows better functioning between different implementations. This command is specially useful in a multi-vendor environment. The ABR types are:

- Cisco ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached and one of them is a backbone area.
- Standard ABR Type: By this definition, a router is considered an ABR if it has more than one area actively attached.
- IBM ARB Type: By this definition, a router is considered an ABR if it has more than one area actively attached and the backbone area is configured. In this case, the configured backbone does not need to be actively connected.
- Shortcut ABR Type: By this definition, the Shortcut ABR is an improvement over the standard ABR behavior by modifying the calculation of inter-area routes. It is allowed to install inter-area routes through non-backbone areas if the non-backbone path is better, thus providing a shortcut through these areas. To prevent routing loops, the inter-area routes are readvertised only if they are associated with the backbone area.

Use the no form of this command to revert the ABR type to the default setting which is "cisco."

Command Mode

Router mode

Example

The following commands set the ABR type to "IBM:"

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)# ospf abr-type ibm
```

Related Commands

none

OVERFLOW DATABASE

Syntax

```
overflow database <0-4294967294> hard|soft

no overflow database
```

Parameters

<0-4294967294>	Indicates the maximum number of LSAs.
hard	Indicates that a shutdown occurs if the number of LSAs exceeds the specified value.
soft	Indicates a warning message appears if the number of LSAs exceeds the specified value.

Description

Use the OVERFLOW DATABASE command to limit the maximum number of LSAs that can be supported by the current OSPF instance. Specify a database value of 0 to 4,294,967,294.

Use the hard parameter with this command if a shutdown is required when the number of LSAs exceeds the specified number. Use the soft parameter with this command if a shutdown is not required, but a warning message is required when the number of LSAs exceeds the specified number.

Use the no form of this command to set no limit on the maximum number of LSAs.

Command Mode

Router mode

Example

The following example sets the database overflow to 5 and a shutdown to occur, if the number of LSAs exceeds 5:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)# overflow database 5 hard
```

Related Commands

none

OVERFLOW DATABASE EXTERNAL

Syntax

```
overflow database external MAXDBSIZE <0-2147483647>
WAITTIME <0-65535>

no overflow database external
```

Parameters

MAXDBSIZE	Specifies the maximum size of an external database. Note that this value should be the same on all routers in the Autonomous System (AS). Choose a value between 0 and 2,147,483,647.
WAITTIME	Specifies the number of seconds the router waits before trying to exit the database overflow state. Choose a value between 0 and 65,535. If this parameter is 0, the router exits the overflow state only after an explicit administrator command.

Description

Use the OVERFLOW DATABASE command to configure the size of the external database and the time the router waits before it tries to exit the overflow state.

Use this command to limit the number of AS-external-LSAs a router can receive when it is in the wait state. It takes the number of seconds specified by the WAITTIME parameter to recover from this state.

Use the no form of this command to reset it to its default value.

Command Mode

Router mode

Example

The following example sets the size of the database overflow to 5 and the time to recover from the overflow state to 3 seconds:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)# overflow database external 5 3
```

Related Commands

none

PASSIVE-INTERFACE

Syntax

```
passive-interface INTERFACENAME A.B.C.D
```

Parameter

INTERFACENAME	Specifies the name of the interface.
A.B.C.D	Specifies the IP address of the interface.

Description

Use the PASSIVE-INTERFACE command to suppress routing updates on the specified interface.

This command is used to configure OSPF on simplex Ethernet interfaces. Since the simplex interfaces represent only one network segment between two devices, configure the transmitting interface as a passive interface. This ensures that OSPF does not send hello packets for the transmitting interface. Both of the devices can see each other via the hello packet generated for the receiving interface.

Command Mode

Router mode

Example

The following commands suppress hello packets on interface 7:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)# passive-interface xe7
```

Related Commands

none

REFRESH TIMER

Syntax

```
refresh timer TIMERVALUE

no network area
```

Parameters

TIMERVALUE	Specifies a timer value in seconds. The default refresh time is 10 seconds. Choose a value between 10 and 1,800 seconds.

Description

Use the REFRESH TIMER command to adjust refresh parameters.

As per RFC 2328 (OSPFv2) in the Architectural Constants section, OSPF requires each LSA to be refreshed by the originating router in every 30 minutes. The REFRESH TIMER command allows you to set the time interval for LSAs to be refreshed. This is in addition to the default refresh time of 30 minutes. For example, if the refresh timer value is set to 20 seconds, the OSPF daemon checks the max-age of LSAs after every 20 seconds and sends a request for refreshing LSAs that are reaching their max-age. Then the OSPF daemon refreshes the specified LSAs in the request, but keeps sending self-originating LSAs every 30 minutes.

Use the no form of this command to disable this function.

Command Mode

Router mode

Example

The following commands assigns the refresh parameters to 40 seconds:

```
switch#configure terminal

switch(config)#refresh area 40
```

Related Commands

none

ROUTER OSPF

Syntax

```
router ospf PROCESSID <1-65535>

no router ospf PROCESSID
```

Parameters

PROCESSID	Indicates any positive integer that identifies a routing process. The value for this parameter must be unique for each routing process. Choose a value between 1 and 65,535.

Description

Use the ROUTER OSPF command to enter the Router mode and to configure an OSPF routing process. Once you enter the Router mode, the prompt changes to indicate a new mode. Specify the Process ID parameter to configure multiple instances. By default, no routing process is defined.

The Process ID of OSPF is an optional parameter. When running a single instance of OSPF, you are not required to specify the Process ID. However, to run multiple instances of OSPF you must specify the Process ID.

Use the no form of this command to terminate an OSPF routing process. The process ID must be a unique value for each routing process.

Command Mode

Configuration Terminal mode

Example

The following example accesses the Router mode and shows the change to the prompt to indicate the new mode:

```
switch#configure terminal

switch(config)#router ospf 100

switch(config-router)#
```

Related Commands

none

SUMMARY-ADDRESS

Syntax

```
summary address A.B.C.D/M (not-advertise)
(tag <0-4294967295>)

no summary address
```

Parameters

A.B.C.D/M	Specifies the range of addresses given as IPv4 starting address and a mask indicating the range.
not-advertise	Suppresses external routes. This is an optional parameter.
tag	The default tag value is 0. Enter a value between 0 and 4,294,967,295. This is an optional parameter.

Description

Use the SUMMARY-ADDRESS command to summarize or suppress external routes with the specified address range.

An address range is a pairing of an address and a mask that is almost the same as an IP network number. For example, if the specified address range is 192.168.0.0/255.255.240.0, it matches: 192.168.1.0/24, 192.168.4.0/22,192.168.8.128/25 and so on.

Redistributing routes from other protocols into OSPF requires the router to advertise each route individually in an external LSA. Use the SUMMARY-ADDRESS command to advertise one summary route for all of the redistributed routes covered by a specified network address and mask. This helps decrease the size of the OSPF link state database.

Command Mode

Router mode

Example

The following example uses the SUMMARY-ADDRESS command to aggregate external LSAs that match the network 172.16.0.0/24 and assign a tag value of 3:

```
switch# configure terminal

switch(config)# router ospf 100
```

```
switch(config-router)# summary-address 172.16.0.0/16
tag 3
```

Related Commands

none

TIMERS SPF

Syntax

```
timers spf SPF-DELAY <0-2147483647> SPF-HOLDTIME <0-
2147483647>

no timers spf SPF-DELAY <0-2147483647> SPF-HOLDTIME
<0-2147483647>
```

Parameters

SPF-DELAY	Specifies the delay between receiving a change to the Shortest Path First (SPF) calculation. Choose a value between 0 and 2,147,483,647. The default value is 5 seconds.
SPF-HOLDTIME	Specifies the hold time between consecutive SPF calculations. Choose a value between 0 and 2,147,483,647. The default value is 10 seconds.

Description

Use the TIMERS SPF command to adjust route-calculation timers. This command configures the delay time between the receipt of a topology change and the calculation of the SPF. This command also configures the hold time between two consecutive SPF calculations.

Use the no form of this command to return the timers to their default values.

Command Mode

Router mode

Example

The following commands set the delay time to 5 seconds and the hold time to 10 seconds:

```
switch# configure terminal

switch(config)# router ospf 100

switch(config-router)# timers spf 5 10
```

Related Commands

none

Chapter 16

Line Mode Commands

This chapter provides a description of the Line mode commands which apply to the serial port on the switch. There are two types of line mode commands: VTY and CONSOLE commands. The VTY commands apply to a Telnet session. The CONSOLE commands apply to the console connected to the switch through the serial port.

This chapter contains the following commands:

EXEC-TIMEOUT

Syntax

```
exec-timeout minutes <0-35791> seconds <0-2147483>

no exec-timeout
```

Parameters

minutes	Specifies the timeout value in minutes. Enter a value between 0 and 35,791 minutes.
seconds	Specifies the timeout value in seconds. Enter a value between 0 and 2,147,483 seconds.

Description

Use the EXEC-TIMEOUT command to set the interval the command interpreter waits for user input detected. A value of 0 minutes and 0 seconds setting causes the Telnet session to wait indefinitely.

Use the no form of this command to disable the wait interval.

Command Mode

Line mode

Example

The following command sets the timer so the Telnet session times out after 2 minutes and 30 seconds if there is no response from the user:

```
switch#configure terminal

switch(config)#line vty 23 66

switch(config-line)#exec-timeout 2 30
```

Related Commands

“SHOW RUNNING-CONFIG” on page 64

LINE CONSOLE

Syntax

```
line console 0
```

Parameters

console — Specifies the primary terminal line. Choose from the following options:

- 0 — Indicates the first line number.

Description

The LINE CONSOLE command sets the primary terminal line. After you enter this command, the prompt changes to indicate the Line mode.

Command Mode

Configuration Terminal mode

Example

The following commands set the first line of the console to 0:

```
switch#configure terminal

switch(config)#line console 0

switch(config-line)#
```

Related Commands

none

PRIVILEGE

Syntax

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

Parameters

level Specifies the privilege level. Choose from the following:

<1 - 15> Specifies a privilege level for a line mode.

Description

The PRIVILEGE command sets the level of access to the AT-S83 commands. Privilege levels 1 through 14 indicate an operator permission level. As an operator, a user has limited right to commands. Only the SHOW, HELP, and LOGOUT commands are available to a user with operator privileges. Privilege level 15 indicates a manager (or system administrator) permission level. A manager has access to all of the commands on the system.

Command Mode

Configuration Terminal mode

Example

The following command sets the privilege level to 1:

```
switch#configure terminal

switch(config)#line console 0

switch(config-line)#privilege 1
```

Related Commands

none

Chapter 17
VLAN Commands

This chapter provides descriptions of the VLAN commands that are available from the View, Privileged Executive, and VLAN Configuration modes.

This chapter contains the following commands:

For configuration information about VLANs, see “Configuring VLANs” on page 371.

SHOW INTERFACE VLAN

Syntax

```
show interface VLANID
```

Parameters

VLANID	Specifies the number of a VLAN. All of the interfaces are members of VLAN1 which is the default VLAN.

Description

Use this command to display information about a particular VLAN by specifying the VLAN ID.

Command Mode

Privileged Executive mode

Example

The following example displays the command and its resulting output:

```
switch# show interface vlan1

Interface vlan1
Scope: both
Hardware is VLAN, address is 0004.2104.0802 (bia
0004.2104.0802)
index 5 metric 1 mtu 1500 duplex-half arp ageing
timeout 600
speed 10000M
<UP,BROADCAST,RUNNING,MULTICAST>
VRF Binding: Not bound
DHCP client is disabled
inet 11.1.1.2/8 broadcast 11.255.255.255
inet6 fe80::210:3ff:fe56:3c03/64
input packets 01, bytes 0154, dropped 00, multicast
packets 0231
output packets 0231, bytes 015518, multicast packets
0231 broadcast packets 01
```

Related Commands

“SHOW VLAN” on page 361

SHOW VLAN

Syntax

```
show vlan all|brief|static|dyanmic VLANID <2-4094>
```

Parameters

vlan — Specifies the type of VLAN to display. Select from the following options:

- all — Displays all types of VLANs in expanded format.
- brief — Displays all types of VLANs in abbreviated format.
- static — Displays information about static VLANs.
- dynamic — Displays information about dynamic VLANs.

VLANID — Enter the VLAN ID. The range is from 2 to 4,094.

Description

Use the SHOW VLAN command to display information about a VLAN by specifying the VLAN ID. The default VLAN, or native VLAN, is VLAN 1.

Command Mode

View and Privileged Executive modes

Example

The following example displays the command and its resulting output:

```
switch# configure terminal

switch# show vlan all
```

VLAN ID	Name	Type	State	Member ports ([u] Untagged), ([t]-Tagged)
2	VLAN0002	STATIC	ACTIVE	xe1(u) xe2(u) xe3(u) xe4 (u) xe5(u) xe6(u) xe7(u) xe8(u)

Related Commands

“SHOW INTERFACE VLAN” on page 360

VLAN

Syntax

```
vlan VLANID name NAME state STATE disable|enable

no vlan VLANID
```

Parameters

VLANID Specifies the ID of the VLAN. Enter a value between 2 and 4094. The default VLAN has an ID of 1.

NAME Specifies the ASCII name of the VLAN.

STATE Specifies the state of the VLAN. Choose from the following:

- disable Indicates the VLAN is disabled.
- enable Indicates the VLAN is enabled.

Description

Use the VLAN command to create a VLAN. In addition, use this command to name a VLAN as well as enable or disable it. To reset the specified VLAN, use the no form of this command.

Command Mode

VLAN Configuration mode

Example

The following commands create a VLAN with a VLAN ID of 2, a name of "myvlan," with an enabled state:

```
switch# configure terminal

switch(config)# vlan database

switch(config-vlan)# vlan 2 name myvlan state enable
```

Related Commands

"VLAN DATABASE" on page 364, "VLAN NAME" on page 365, and "VLAN STATE" on page 366

VLAN DATABASE

Syntax

```
vlan database
```

Parameters

none

Command Mode

Configuration Terminal mode

Description

Use the VLAN DATABASE command to enter the VLAN configuration mode. After you enter the VLAN mode, the prompt changes to indicate the new mode and you can enter commands to add, delete, or modify values associated with a single VLAN.

Example

The following example permits access to the VLAN Configuration mode and shows the change to prompt that indicates the new mode:

```
switch# configure terminal

switch(config)# vlan database

switch(config-vlan)#
```

Related Commands

“VLAN” on page 363

VLAN NAME

Syntax

```
vlan pvid <2-4094> name NAME
```

Parameters

pvid	Enter the VLAN ID of the VLAN. The range is from 2 to 4094. You cannot assign a name to VLAN 1 which is the default VLAN.
NAME	Enter the name of the VLAN. The range is from 1 to 24 alphanumeric characters. Special characters, such as "_," "?," and "*"are permitted.

Command Mode

VLAN Configuration mode

Description

Use the VLAN NAME command to assign a name to a VLAN.

Examples

In the following example, VLAN 4 is assigned the name "vlan 4 stre:"

```
switch# configure terminal

switch(config)# vlan database

switch(config-vlan)# vlan 4 name "vlan 4 stre"
```

Related Commands

none

VLAN STATE

Syntax

```
vlan VLANID state enable|disable
```

Parameters

VLANID	Specifies the ID of the VLAN. Enter a value between 2 and 4094. The default VLAN has an ID of 1.
state	Indicates the state of the VLAN is either enabled or disabled. Choose from the following:
	enable — Specifies the VLAN is enabled.
	disable — Specifies the VLAN is disabled.

Description

Use this command to set the operational state of the VLAN.

Command Mode

VLAN Configuration mode

Examples

In the following commands disable VLAN 3:

```
switch# configure terminal
switch(config)# vlan database
switch(config-vlan)# vlan 3 state disable
```

Related Commands

none

Chapter 18

Sample Configurations

This chapter contains sample configurations of the following protocols:

Configuring 802.1x Access Control

The IEEE 802.1x Access Control specification restricts unauthenticated devices from connecting to the switch. After authentication is successful, traffic is permitted through the switch.

In the following configuration example, the RADIUS server keeps the client information, validating the identity of the client and updating the switch regarding the authentication of the client. The switch provides the physical connection between two clients on interface 1 and 2, and the server, interface 3. The switch requests information from the client and relays the information to the server. Then the switch relays the information to the client.

To configure 802.1x authentication, first enable authentication on interfaces 1 and 2. Then specify the RADIUS server IP address on interface 3. Perform the following procedure to configure 802.1x Access Control on the switch:

1. Enter the Configuration Terminal mode:

   ```
   switch# configure terminal
   ```

2. Enable authentication globally on the switch:

   ```
   switch(config)# dot1x system-auth-ctrl
   ```

3. Enter the Interface mode and configure interface 1:

   ```
   switch(config)#interface xe1
   ```

4. Enable authentication with RADIUS on interface 1:

   ```
   switch(config-if)# dot1x port-control auto
   ```

5. Configure interface 2:

   ```
   switch(config-if)#interface xe2
   ```

6. Enables authentication with RADIUS on interface 2.

   ```
   switch(config-if)# dot1x port-control auto
   ```

7. Exit the Interface mode and enter the Configuration Terminal mode:

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

8. Specify the IP address of the RADIUS server:

   ```
   switch(config)#radius-server host 192.126.12.1
   ```

9. Specify the shared key "ipi" between the RADIUS server and the client:

   ```
   switch(config)#radius-server key ipi
   ```

10. Enter the Interface mode and configure interface 3:

    ```
    switch(config)# interface xe3
    ```

11. Sets the IP address on interface 3.

    ```
    switch(config-if)# ip address 192.126.12.0
    ```

Configuring NTP Authentication

For information about the NTP authentication commands, see Chapter 6, “Configuration Terminal Mode Commands” on page 105. To configure NTP authentication, do the following:

1. Enter the Configuration Terminal mode:

   ```
   configure terminal
   ```

2. Enable NTP authentication on the switch:

   ```
   ntp authenticate
   ```

3. Define an authentication key. In the following example, the key number is “777,” the authentication type is MD5, and the key name is “authkey777:”

   ```
   ntp authentication key 777 md5 authkey777
   ```

   You may define multiple authentication keys.

   Make sure the authentication key is synchronized with an external device.

4. Specify a key number that you have previously defined with the NTP AUTHENTICATION KEY command:

   ```
   ntp trusted-key 777
   ```

Configuring VLANs

A Virtual Local Area Network (VLAN) is a network topology that is configured according to a logical scheme rather than the physical layout. VLANs can be used to combine any collection of LAN segments into an autonomous user group that appears as a single LAN. In addition, VLANs logically segment the network into different broadcast domains so that packets are forwarded only between interfaces within the VLAN. In general, a VLAN corresponds to a particular subnet.

To configure a VLAN, you create a VLAN in the configuration VLAN mode. Then enter the Interface mode which allows you to assign a VLAN to a interface. There are two VLAN modes:

- Access mode - permits you to assign one VLAN to one interface
- Trunk mode - permits you to assign multiple VLANs to one interface

The default VLAN, which is also the native VLAN, is VLAN 1. In the following configuration example, Use the sample VLAN configuration to:

- Access the VLAN mode
- Create VLANs 2 through 4
- Assign a name to a VLAN
- Assign an interface to a VLAN

1. Enter the Configuration Terminal mode:

   ```
   switch# configure terminal
   ```

2. Enter the VLAN mode:

   ```
   switch(config)#vlan database
   ```

3. Create VLAN 2:

   ```
   switch(config-vlan)#vlan 2
   ```

   By default, VLAN 2 is enabled.

4. Assign VLAN 2 the name "stre:"

   ```
   switch(config-vlan)#vlan 2 name stre
   ```

5. Create VLAN 3.

   ```
   switch(config-vlan)#vlan 3
   ```

   By default, VLAN 3 is enabled.

6. Create VLAN 4.

   ```
   switch(config-vlan)#vlan 4
   ```

   By default, VLAN 4 is enabled.

7. Exit the VLAN mode and enter the Configuration Terminal mode:

   ```
   switch(config-vlan)#exit
   ```

8. Enter the Interface mode and configure interface 1:

   ```
   switch(config-vlan)#interface xe1
   ```

   The commands following this command apply to interface 1 only.

9. Assign interface 1 to access mode which permits a single untagged VLAN:

   ```
   switch(config-if)# switchport mode access
   ```

10. Assign VLAN 4 to access mode on interface 1:

    ```
    switch(config-if)# switchport access vlan 4
    ```

    This is an untagged VLAN.

11. Exit the VLAN mode and enter the Configuration Terminal mode:

    ```
    switch(config-vlan)#exit
    ```

12. Enter the Interface mode and configure interface 2:

    ```
    switch(config)# interface xe2
    ```

    The commands following this command apply to this interface only.

13. Assigns VLAN 4 to interface 2.

    ```
    switch(config-if)#switch access vlan 4
    ```

    This is an untagged VLAN.

14. Exit the VLAN mode and enter the Configuration Terminal mode:

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

15. Enter the Interface mode and configure interface 3:

    ```
    switch(config)#interface xe3
    ```

    The commands following this command apply to this interface.

16. Enter the trunk mode which allows you to assign multiple interfaces to one VLAN:

    ```
    switch(config-if)#switchport mode trunk
    ```

17. Assign VLAN 3 to interface 3:

    ```
    switch(config-if)# switchport access vlan 3
    ```

Index

D

E

F

Q

R

T

U

V

W