Management Software

AT-S63

Command Line User's Guide

For Stand-alone AT-9400 Switches and AT-9400Ts Stacks

AT-S63 Version 2.2.0 for Layer 2+ AT-9400 Switches
AT-S63 Version 4.1.0 for Basic Layer 3 AT-9400 Switches

613-001024 Rev. C

Allied Telesis™

Allied Telesis, Inc. reserves the right to make changes in specifications and other information contained in this document without prior written notice. The information provided herein is subject to change without notice. In no event shall Allied Telesis, Inc. be liable for any incidental, special, indirect, or consequential damages whatsoever, including but not limited to lost profits, arising out of or related to this manual or the information contained herein, even if Allied Telesis, Inc. has been advised of, known, or should have known, the possibility of such damages.

Contents

Tables

Preface

This guide describes the standard command line interface and the AlliedWare Plus™ command interface in the AT-S63 Management Software for the AT-9400 Gigabit Ethernet Switches.

This Preface contains the following sections:

⚠ **Caution**

The software described in this documentation contains certain cryptographic functionality and its export is restricted by U.S. law. As of this writing, it has been submitted for review as a "retail encryption item" in accordance with the Export Administration Regulations, 15 C.F.R. Part 730-772, promulgated by the U.S. Department of Commerce, and conditionally may be exported in accordance with the pertinent terms of License Exception ENC (described in 15 C.F.R. Part 740.17). In no case may it be exported to Cuba, Iran, Iraq, Libya, North Korea, Sudan, or Syria. If you wish to transfer this software outside the United States or Canada, please contact your local Allied Telesis sales representative for current information on this product's export status.

How This Guide is Organized

This guide has the following sections and chapters:

- Section I: Basic Operations

  Chapter 1, “Overview” on page 31

  Chapter 2, “Basic Command Line Commands” on page 53

  Chapter 3, “Basic Switch Commands” on page 65

  Chapter 4, “AT-9400Ts Stack Commands” on page 103

  Chapter 5, “Enhanced Stacking Commands” on page 109

  Chapter 6, “Simple Network Time Protocol (SNTP) Commands” on page 117

  Chapter 7, “SNMPv1 and SNMPv2c Commands” on page 129

  Chapter 8, “Port Parameter Commands” on page 151

  Chapter 9, “Port Statistics Commands” on page 185

  Chapter 10, “MAC Address Table Commands” on page 191

  Chapter 11, “Static Port Trunking Commands” on page 205

  Chapter 12, “LACP Port Trunking Commands” on page 219

  Chapter 13, “Port Mirroring Commands” on page 237

  Chapter 14, “Link-flap Protection Commands” on page 243

- Section II: Advanced Operations

  Chapter 15, “File System Commands” on page 255

  Chapter 16, “File Download and Upload Commands” on page 275

  Chapter 17, “Event Log and Syslog Client Commands” on page 303

  Chapter 18, “Classifier Commands” on page 335

  Chapter 19, “Access Control List Commands” on page 347

  Chapter 20, “Class of Service (CoS) Commands” on page 361

  Chapter 21, “Quality of Service (QoS) Commands” on page 373

  Chapter 22, “Group Link Control Commands” on page 427

  Chapter 23, “Denial of Service Defense Commands” on page 441

  Chapter 24, “Power Over Ethernet Commands” on page 455

- Section III: Snooping Protocols

  Chapter 25, “Internet Group Management Protocol (IGMP) Snooping Commands” on page 467

  Chapter 26, “Internet Group Management Protocol (IGMP) Snooping Querier Commands” on page 479

  Chapter 27, “Multicast Listener Discovery (MLD) Snooping Commands” on page 485

  Chapter 28, “Router Redundancy Protocol (RRP) Snooping Commands” on page 499

  Chapter 29, “Ethernet Protection Switching Ring (EPSR) Snooping Commands” on page 503

- Section IV: SNMPv3

  Chapter 30, “SNMPv3 Commands” on page 509

- Section V: Spanning Tree Protocols

  Chapter 31, “Spanning Tree Protocol (STP) Commands” on page 573

  Chapter 32, “Rapid Spanning Tree Protocol (RSTP) Commands” on page 589

  Chapter 33, “Multiple Spanning Tree Protocol (MSTP) Commands” on page 611

- Section VI: Virtual LANs

  Chapter 34, “Port-based VLAN, Tagged VLAN, and Multiple VLAN Mode Commands” on page 643

  Chapter 35, “GARP VLAN Registration Protocol Commands” on page 663

  Chapter 36, “Protected Ports VLAN Commands” on page 683

  Chapter 37, “MAC Address-based VLAN Commands” on page 693

- Section VII: Routing

  Chapter 38, “Internet Protocol Version 4 Packet Routing Commands” on page 705

  Chapter 39, “BOOTP Relay Commands” on page 757

  Chapter 40, “Virtual Router Redundancy Protocol (VRRP) Commands” on page 765

- Section VIII: Port Security

  Chapter 41, “MAC Address-based Port Security Commands” on page 793

  Chapter 42, “802.1x Port-based Network Access Control Commands” on page 805

- Section IX: Management Security

  Chapter 43, “Web Server Commands” on page 835

  Chapter 44, “Encryption Key Commands” on page 845

  Chapter 45, “Public Key Infrastructure (PKI) Certificate Commands” on page 853

  Chapter 46, “Secure Sockets Layer (SSL) Commands” on page 869

  Chapter 47, “Secure Shell (SSH) Commands” on page 873

  Chapter 48, “TACACS+ and RADIUS Commands” on page 881

  Chapter 49, “Management Access Control List Commands” on page 899

Product Documentation

For overview information on the features of the AT-9400 Switches and the AT-S63 Management Software, refer to:

❒ AT-S63 Management Software Features Guide
(PN 613-001022)

For instructions on how to start local or remote management sessions on stand-alone AT-9400 Switches or AT-9400Ts Stacks, refer to:

❒ Starting an AT-S63 Management Session Guide
(PN 613-001023)

For instructions on how to install or manage stand-alone AT-9400 Switches, refer to:

❒ AT-9400 Gigabit Ethernet Switch Installation Guide
(PN 613-000987)

❒ AT-S63 Management Software Menus User’s Guide
(PN 613-001025)

❒ AT-S63 Management Software Command Line User’s Guide
(PN 613-001024)

❒ AT-S63 Management Software Web Browser User’s Guide
(PN 613-001026)

For instructions on how to install or manage AT-9400Ts Stacks, refer to:

❒ AT-9400Ts Stack Installation Guide
(PN 613-001191

❒ AT-S63 Management Software Command Line User’s Guide
(PN 613-001024)

❒ AT-S63 Management Software Web Browser User’s Guide for AT-9400Ts Stacks
(PN 613-001028)

The installation and user guides for all the 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.

Where to Go First

Allied Telesis recommends that you read Chapter 1, “Overview,” in the *AT-S63 Management Software Features Guide* before you begin to manage the switch for the first time. There you will find a variety of basic information about the unit and the management software, like the two levels of manager access levels and the different types of management sessions. The *AT-S63 Management Software Features Guide* is also your resource for background information on the features of the switch. You can refer there for the relevant concepts and guidelines when configuring a feature for the first time.

Starting a Management Session

For instructions on how to start a local or remote management session on the AT-9400 Switch, refer to the *Starting an AT-S63 Management Session Guide*.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

Caution
Cautions inform you that performing or omitting a specific action may result in equipment damage or loss of data.

Warning
Warnings inform you that performing or omitting a specific action may result in bodily injury.

Contacting Allied Telesis

This section provides Allied Telesis contact information for technical support and for sales and corporate information.

Online Support

You can request technical support online by accessing the Allied Telesis Knowledge Base: **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 at **www.alliedtelesis.com**. Select your country from the list on the web site and then select the appropriate tab.

Returning Products

Products for return or repair must first be assigned a return materials authorization (RMA) number. A product sent to Allied Telesis without an RMA number will be returned to the sender at the sender’s expense. For instructions on how to obtain an RMA number, go to the Support section on our web site at **www.alliedtelesis.com**.

Sales or Corporate Information

You can contact Allied Telesis for sales or corporate information through our web site at **www.alliedtelesis.com**.

Management Software Updates

New releases of the management software for our managed products are available from the following Internet sites:

- ❒ Allied Telesis web site: **www.alliedtelesis.com**
- ❒ Allied Telesis FTP server: **ftp://ftp.alliedtelesis.com**

If the FTP server prompts you to log on, enter “anonymous” as the user name and your email address as the password.

Section I

Basic Operations

This section contains the following chapters:

Chapter 1

Overview

This chapter has the following sections:

Command Line Interfaces

The AT-S63 Management Software has four management interfaces — menus, web browser windows, standard command line, and AlliedWare Plus™ command line. This guide explains the standard command interface and the AlliedWare Plus™ command interface.

The standard command interface is the most comprehensive of all the interfaces because it gives you complete control over all the features and parameters on the switch. Its commands let you set and view the parameters of all the features as well as upload and download files. This interface is available from local management sessions through the terminal port on the switch and from remote management sessions with Telnet and Secure Shell clients, and can be used to manage both stand-alone AT-9400 Switches and AT-9400Ts Stacks.

The AlliedWare Plus interface is new to the AT-S63 Management Software and is based on the AlliedWare Plus operating system featured on other Allied Telesis products, like advanced Layer 3 switches. You may find the commands in this new command line easier and more convenient to use to manage the switch if you are already familiar with the AlliedWare Plus operating system.

This interface is similar to the standard command line interface in several ways. First, you can use it to manage stand-alone AT-9400 Switches and AT-9400Ts Stacks. Second, you can access it locally through the terminal port and remotely with Telnet and Secure Shell clients. In fact, you can switch between the two command line interfaces, as well as the menus interface, from a management session without having to log out and log in again, making it possible for you to use different management interfaces during the same management session.

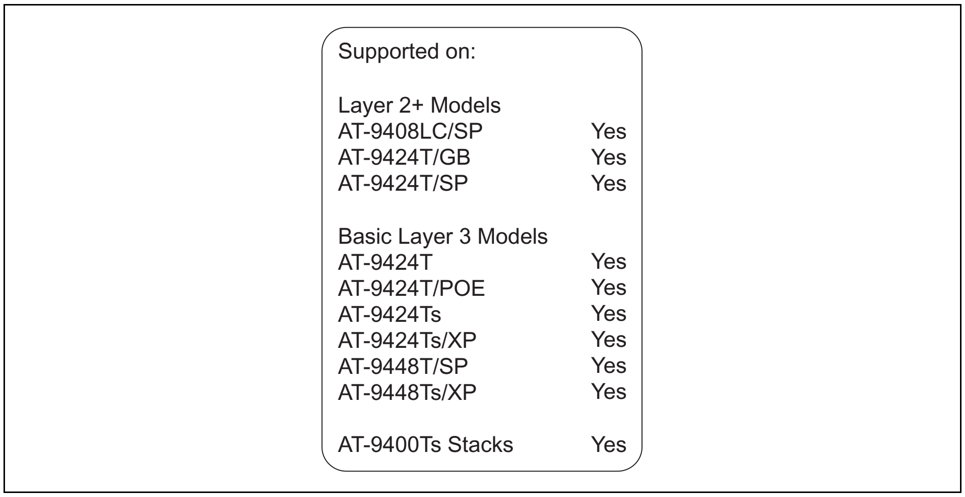
However, there are a couple features you cannot configure with the AlliedWare Plus interface. For those features, you'll have to use a different interface, probably the standard command line interface. Furthermore, this interface handles a few of the features, like classifiers, access control lists and Quality of Service policies, very differently than the other interfaces.

Stand-alone AT-9400 Switches and AT-9400Ts Stacks

You can use the standard command interface and the AlliedWare Plus command line interface to manage stand-alone AT-9400 Switches and AT-9400Ts Stacks. Stacking is only supported on the AT-9424Ts, AT-9424Ts/XP, and AT-9448Ts/XP Switches, and requires the AT-StackXG Stacking Module. For further information, refer to the *AT-S63 Management Software Features User's Guide*.

Supported Features and Switches

You'll find this table on the first page of each chapter. It identifies the switches in the AT-9400 Series that support the feature of the chapter. For further information of the features of the switches, refer to the *AT-S63 Management Software Features Guide*.



Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

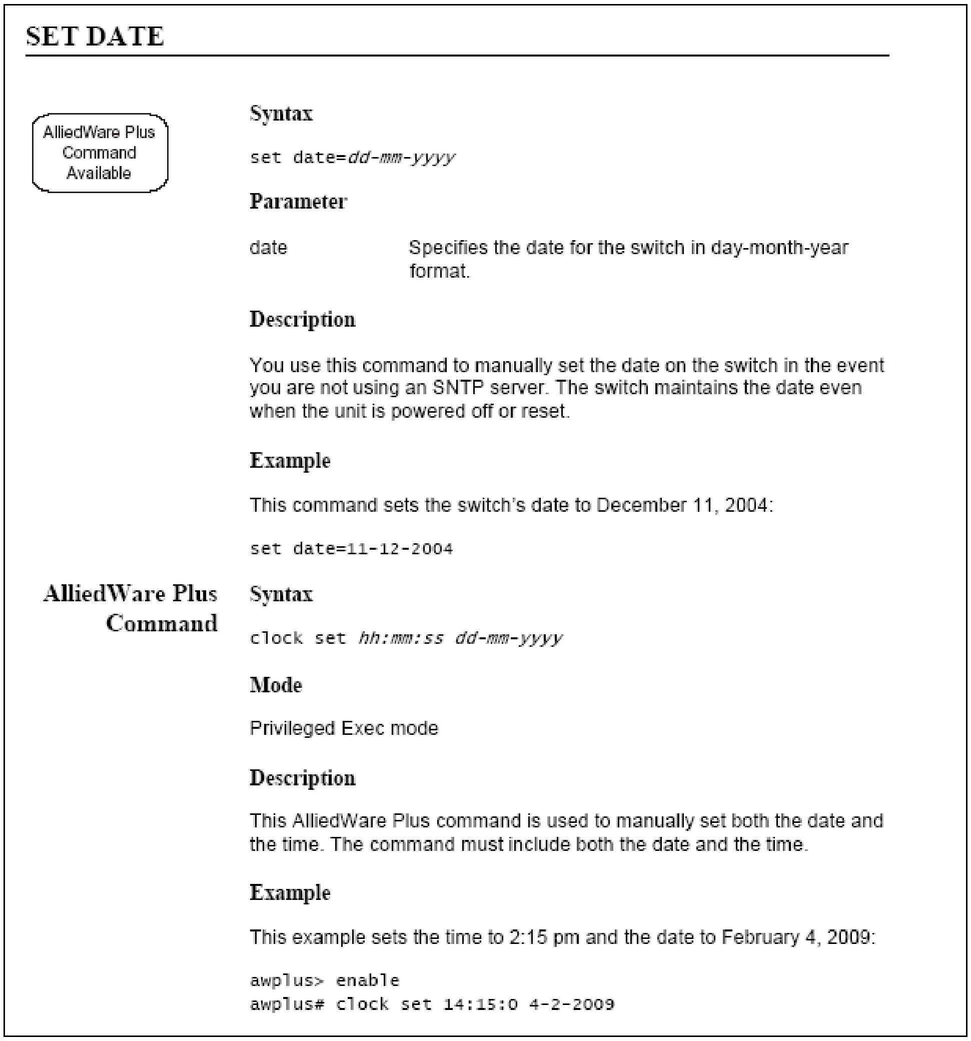
Figure 1. AT-9400 Switch Table

Page Format

In this guide, standard commands that have equivalent AlliedWare Plus commands have this logo at the start of their descriptions.

Figure 2. AlliedWare Plus Command Available Logo

The standard command is described first followed by the equivalent AlliedWare Plus command. In the example in Figure 3, the standard command is SET DATE and the equivalent AlliedWare Plus command is CLOCK SET.



SET DATE

AlliedWare Plus
Command
Available

Syntax

```
set date=dd-mm-yyyy
```

Parameter

date — Specifies the date for the switch in day-month-year format.

Description

You use this command to manually set the date on the switch in the event you are not using an SNTP server. The switch maintains the date even when the unit is powered off or reset.

Example

This command sets the switch’s date to December 11, 2004:

```
set date=11-12-2004
```

AlliedWare Plus Command

Syntax

```
clock set hh:mm:ss dd-mm-yyyy
```

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is used to manually set both the date and the time. The command must include both the date and the time.

Example

This example sets the time to 2:15 pm and the date to February 4, 2009:

```
awplus> enable
awplus# clock set 14:15:0 4-2-2009
```

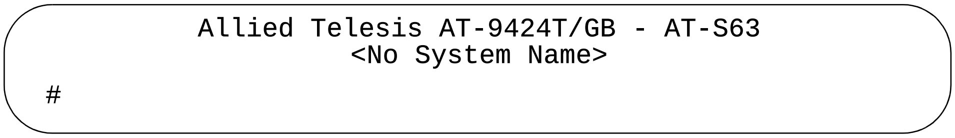
Figure 3. Sample Command Page

Standard Command Line Interface

The standard command interface has a flat structure. You enter all the commands at one level.

The account you use to log on determines the commands you can use. There is a manager account and an operator account. The manager account gives you access to all the commands while the operator account restricts you to commands for viewing the parameter settings.

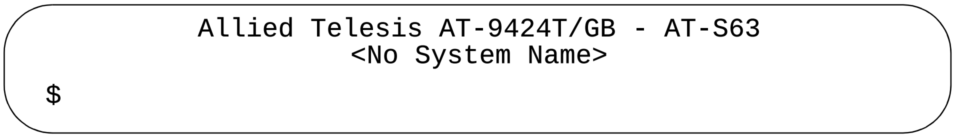
The command prompt indicates whether you logged on as a manager or an operator. If you are a manager, you'll see the "#" prompt.



```
            Allied Telesis AT-9424T/GB - AT-S63
                     <No System Name>
#
```

Figure 4. Manager Command Prompt

If you are an operator, you'll see the "$" prompt.



```
            Allied Telesis AT-9424T/GB - AT-S63
                     <No System Name>
$
```

Figure 5. Operator Command Prompt

AlliedWare Plus™ Command Line Interface

The following sections describe the features and characteristics of the AlliedWare Plus™ interface.

Command Modes

The AlliedWare Plus interface has a very different structure from the standard command interface. Instead of a flat command structure, it has different modes that are arranged in the hierarchy illustrated in Figure 6.

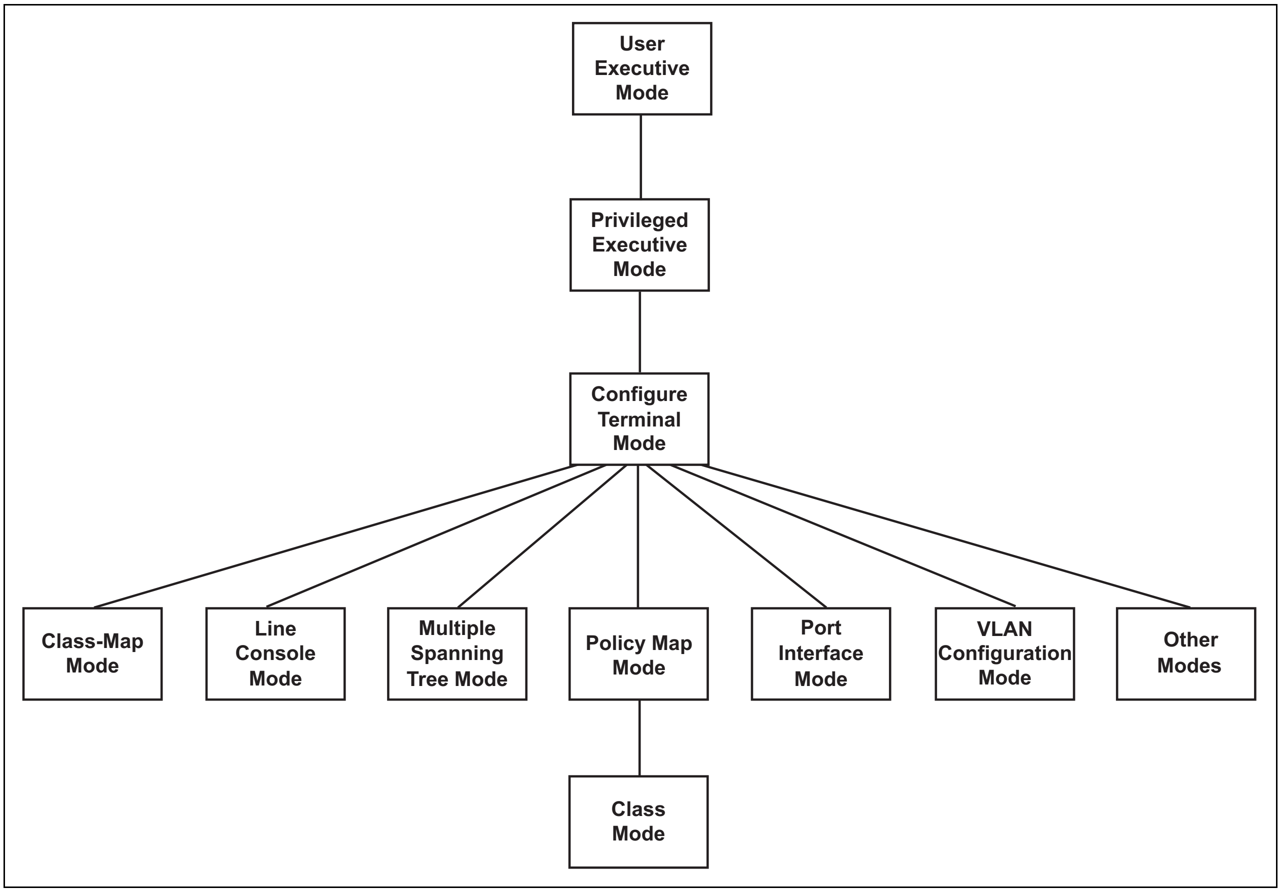


Figure 6. Command Modes

All of the modes have different commands and support different management functions. The only exception is the Privileged Executive mode, which supports all the same functions as the User Executive Mode, plus quite a few others.

Before you can perform a management function, you have to move to the mode that has the appropriate commands. For instance, to configure the parameter settings of the ports on the switch, such as the speeds and duplex modes, you have to go to the Interface mode because that's the mode that has the commands for configuring the port parameters.

In some cases, you might find that you have to use commands in different modes to complete a management function. Creating new VLANs is an example of this because you first have to go to the VLAN Configuration mode to create the VLANs and then to the Port Interface mode to designate their ports.

The modes, their command line prompts, and their functions are listed in Table 1.

Table 1. AlliedWare Plus Modes

Mode	Prompt	Function
User Executive Mode	awplus>	❐ Display the switch settings. ❐ List the files in the file system. ❐ Ping remote systems.
Privileged Executive Mode	awplus#	❐ Display the switch settings ❐ List the files in the file system ❐ Ping remote systems ❐ Set the date and time ❐ Save the current configuration ❐ Download new versions of the AT-S63 Management Software ❐ Restore the default settings ❐ Rename files in the file system ❐ Reset the switch
Configure Terminal Mode	(config)#	❐ Create classifiers and access control lists ❐ Create encryption keys for remote HTTPS and SSH management ❐ Activate and deactivate 802.1x port-based network access control ❐ Assign a name to the switch ❐ Configure IGMP snooping ❐ Set the MAC address table aging timer ❐ Enter static MAC addresses ❐ Specify the IP address of a SNTP server ❐ Configure the RADIUS client ❐ Set the console timer

Table 1. AlliedWare Plus Modes

Mode	Prompt	Function
Class-map Mode	(config-cmap)#	❒ Create classifiers and flow groups for Quality of Service policies
Line Console mode	(config-line)#	❒ Set the console timer ❒ Activate and deactivate the RADIUS or TACACS+ client for manager and operator accounts ❒ Set the baud rate of the terminal port
Multiple Spanning Tree Mode	(config-mst)#	❒ Create multiple spanning tree instances ❒ Specify a region’s name and revision level.
Policy Map mode	(config-pmap)#	❒ Map flow groups to traffic classes for Quality of Service policies
Port Interface Mode	(config-if)#	❒ Configure port settings ❒ Disable and enable ports ❒ Configure port mirroring ❒ Configure 802.1x port-based network access control ❒ Create static port trunks ❒ Add and remove ports from VANs ❒ Create Quality of Service policies
Router mode	(config-router)#	❒ Add RIP to routing interfaces. ❒ Configure virtual routes for VRRP.
Static Port Trunk Interface mode	(config-if)#	❒ Set the load distribution method for static port trunks.
VLAN Configuration mode	(config-vlan)#	❒ Create VLANs
VLAN Interface Mode	(config-if)#	❒ Create a routing interface ❒ Designate the local interface
Class mode	(config-pmap-c)#	❒ Configure traffic classes for Quality of Service policies

Moving Down the Hierarchy

To move down through the hierarchy, you have to move through the modes in sequence. Skipping modes is not allowed.

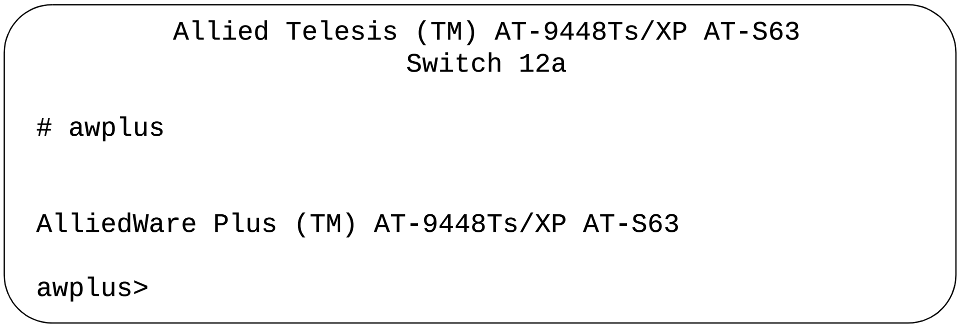
There is a different command for each mode. To move from the User Exec mode to the Privileged Exec mode, for instance, use the ENABLE command. Some of the commands require a value, like the INTERFACE PORT command which must have one or more port numbers and which is used to enter the Port Interface mode.

AWPLUS Command

You use this command at the standard command line prompt to enter the AlliedWare Plus command line interface and the User Exec mode. If you log on as an operator, this is as far in the hierarchy as you can go. To go further, you have to log on as a manager.

The format of the command is:

awplus



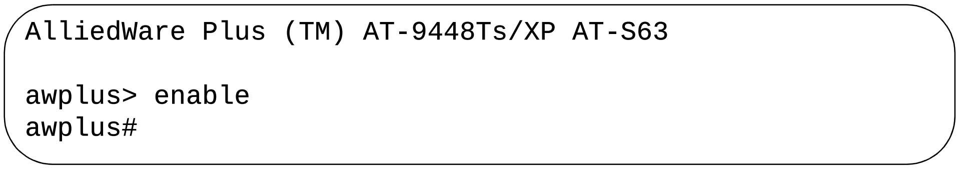
```
          Allied Telesis (TM) AT-9448Ts/XP AT-S63
                         Switch 12a

# awplus


AlliedWare Plus (TM) AT-9448Ts/XP AT-S63

awplus>
```

Figure 7. Using the AWPLUS Command to Start the AlliedWare Plus Command Line Interface

ENABLE Command

You use this command to move from the User Exec mode to the Privileged Exec mode. The format of the command is:

```
enable
```



```
AlliedWare Plus (TM) AT-9448Ts/XP AT-S63

awplus> enable
awplus#
```

Figure 8. Moving from the User Exec Mode to the Privileged Exec Mode with the ENABLE Command

CONFIGURE TERMINAL Command

You use this command to move from the Privileged Exec mode to the Configure Terminal mode. The format of the command is:

```
configure terminal
```

```
AlliedWare Plus (TM) AT-9448Ts/XP AT-S63

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

Figure 9. Moving from the Privileged Exec Mode to the Configure Terminal Mode with the CONFIGURE TERMINAL Command

CLASS-MAP Command

You use this command to move from the Configure Terminal mode to the Class-Map mode to create classifiers and flow groups for Quality of Service policies. The format of the command is:

```
class-map id_number
```

```
awplus(config)# class-map 256
awplus(config-cmap)#
```

Figure 10. Moving from the Configure Terminal Mode to the Class Map Mode with the CLASS-MAP Command

LINE CONSOLE 0 Command

You use this command to move from the Configure Terminal mode to the Line Console mode to set the console timer, activate or deactivate remote authentication of manager accounts, and set the baud rate of the terminal port. The format of the command is:

```
line console 0
```

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

Figure 11. Moving from the Configure Terminal Mode to the Line Console Mode with the LINE CONSOLE Command

SPANNING-TREE MST CONFIGURATION Command

You use this command to move from the Configure Terminal mode to the Multiple Spanning Tree mode to create multiple spanning tree instances. The format of the command is:

```
spanning-tree mst configuration
```

```
awplus(config)# spanning-tree mst configuration
awplus(config-mst)#
```

Figure 12. Moving from the Configure Terminal Mode to the Multiple Spanning Tree Mode with the SPANNING-TREE MST CONFIGURATION Command

POLICY-MAP Command

You use this command to move from the Configure Terminal mode to the Policy Map mode where flow groups are mapped to traffic classes for Quality of Service policies. The format of the command is:

```
policy-map id_number
```

```
awplus(config)# policy-map 1
awplus(config-pmap)#
```

Figure 13. Moving from the Configure Terminal Mode to the Line Console Mode with the LINE CONSOLE Command

CLASS Command

You use this command to move from the Policy Map mode to the Class mode, to configure the traffic classes for Quality of Service policies. The format of the command is:

```
class id_number
```

This example enters the Class mode for the traffic class with the ID number 1:

```
awplus(config-pmap)# class 1
awplus(config-pmap-c)#
```

Figure 14. Moving from the Configure Terminal Mode to the Class Mode with the CLASS Command

INTERFACE PORT Command

You use this command to move from the Configure Terminal mode to the Port Interface mode where you configure the parameter settings of the ports and add ports to VLANs and Quality of Service policies. The format of the command is:

`interface` *`port`*

This example enters the Interface mode for port 21.

```
awplus(config)# interface 21
awplus(config-if)#
```

Figure 15. Moving from the Configure Terminal Mode to the Port Interface Mode with the INTERFACE PORT Command

You can specify more than one port in the command to configure more than one port at a time. This example enters the Interface mode for ports 11 to 15 and 22.

```
awplus(config)# interface 11-15,22
awplus(config-if)#
```

Figure 16. Specifying More Than One Port in the NTERFACE PORT Command

The INTERFACE PORT command is also located in the Port Interface mode so you don’t have to return to the Configure Terminal mode to configure a different port. This example moves from the current Port Interface mode to the Port Interface mode for ports 7 and 10.

```
awplus(config-if)# interface 7,10
awplus(config-if)#
```

Figure 17. Moving within the Port Interface Mode with the INTERFACE Command

VLAN DATABASE Command

You use this command to move from the Configure Terminal mode to the VLAN Configuration mode which you use to create VLANs. The format of the command is:

```
vlan database
```

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

Figure 18. Moving from the Configure Terminal Mode to the VLAN DATABASE Mode with the LINE CONSOLE Command

INTERFACE VLAN Command

You use this command to move from the Configure Terminal mode to the VLAN Interface mode to create routing interfaces and to designate the local interface. You can specify only one VLAN and the VLAN must be indicated by its name and not by its VID. The format of the command is:

`interface` *`vlan_name`*

This example enters the VLAN Interface mode for the Sales VLAN.

```
awplus(config)# interface Sales
awplus(config-if)#
```

Figure 19. Moving from the Configure Terminal Mode to the VLAN Interface Mode with the INTERFACE VLAN Command

This example enters the VLAN Interface mode for the Default_VLAN.

```
awplus(config)# interface default_vlan
awplus(config-if)#
```

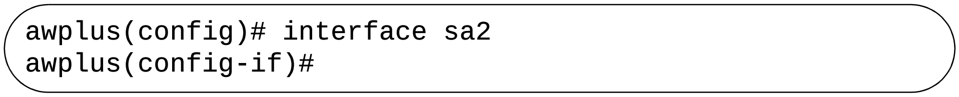
Figure 20. Moving from the Configure Terminal Mode to the VLAN Interface Mode with the INTERFACE VLAN Command

INTERFACE TRUNK Command

You use this command to move from the Configure Terminal mode to the Static Port Trunk Interface mode, to change the load distribution methods of static port trunks. You specify a trunk by its name of “sa” followed by its ID number. You can specify only one static port trunk at a time. The format of the command is:

`interface` *`trunk_name`*

This example enters the Static Port Trunk Interface mode for a trunk with the name “sa2:”



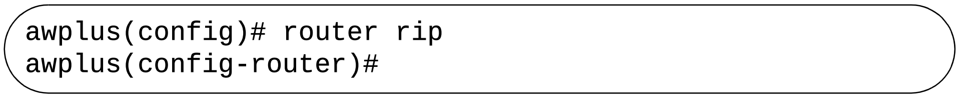
```
awplus(config)# interface sa2
awplus(config-if)#
```

Figure 21. Moving from the Configure Terminal Mode to the Static Port Trunk Interface Mode with the INTERFACE TRUNK Command

ROUTER RIP Command

You use this command to move from the Configure Terminal mode to the Router mode, in which you add RIP to routing interfaces and configure the protocol settings. The format of the command is:

```
router rip
```



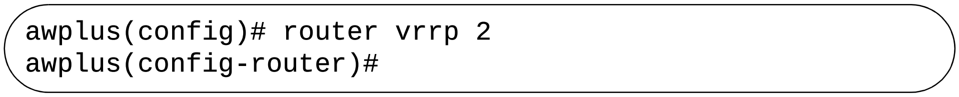
```
awplus(config)# router rip
awplus(config-router)#
```

Figure 22. Moving from the Configure Terminal Mode to the Router Mode with the ROUTER RIP Command

ROUTER VRRP Command

You use this command to move from the Configure Terminal mode to the Router mode, to configure virtual routes for VRRP. The format of the command is:

router vrrp *vrid*



```
awplus(config)# router vrrp 2
awplus(config-router)#
```

Figure 23. Moving from the Configure Terminal Mode to the Router Mode with the ROUTER VRRP Command

Moving Up the Hierarchy

To move up the mode hierarchy, you use the EXIT command and the END command.

EXIT Command

This command is available in all the modes. When you enter this command at the User Exec mode or the Privileged Exec mode, you exit from the AlliedWare Plus command interface and return to the standard command line interface. The same command entered at any of the other modes moves you up one level in the hierarchy, as illustrated in Figure 24.

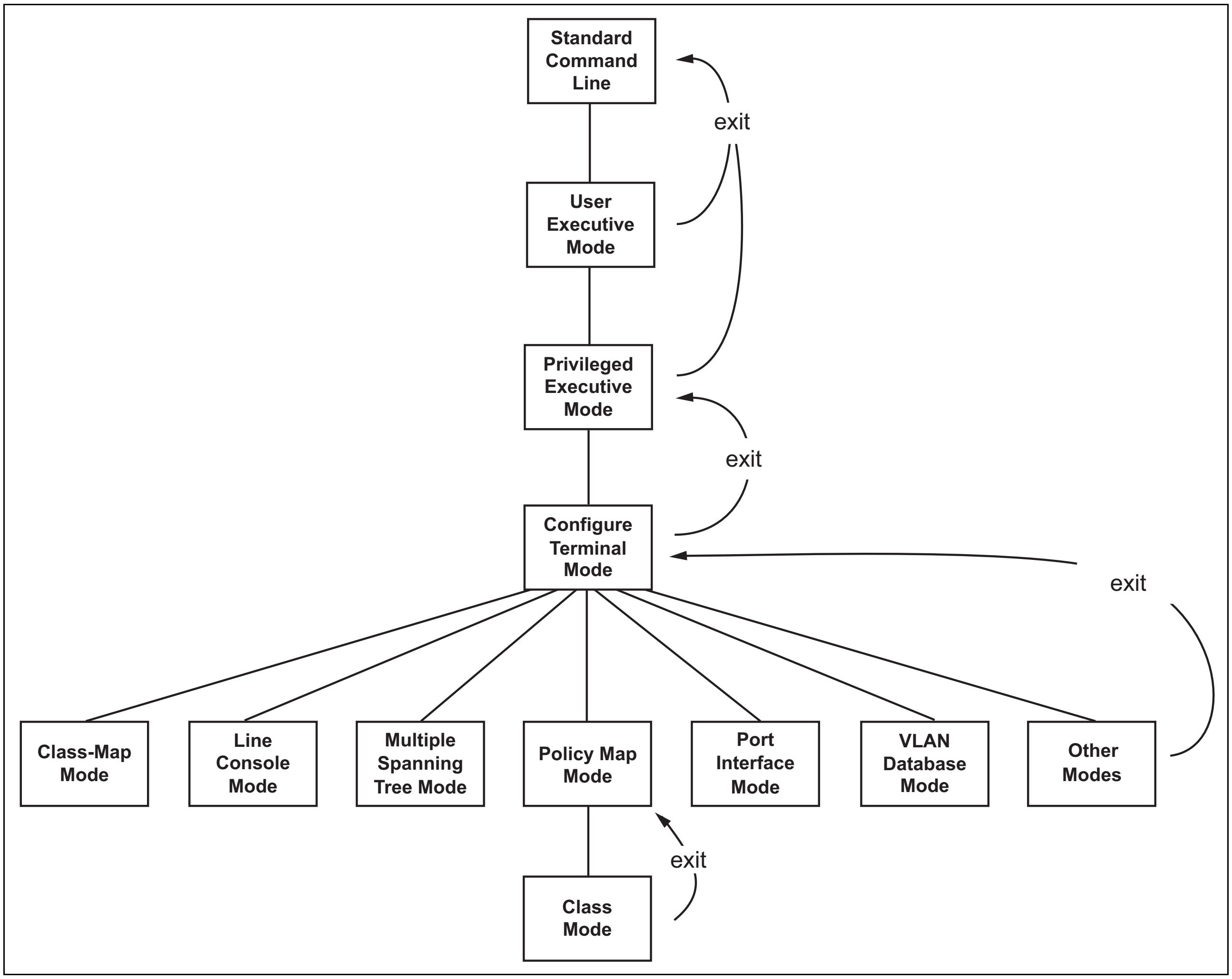


Figure 24. Moving Up One Mode with the EXIT Command

END Command

After configuring a feature, you'll probably want to use the SHOW commands in the User Exec mode or the Privileged Exec mode to verify your changes. While you could move back through the modes with the EXIT command, you may find the END command more convenient because it jumps you directly to the Privileged Exec mode from any of the modes below the Configure Terminal mode.

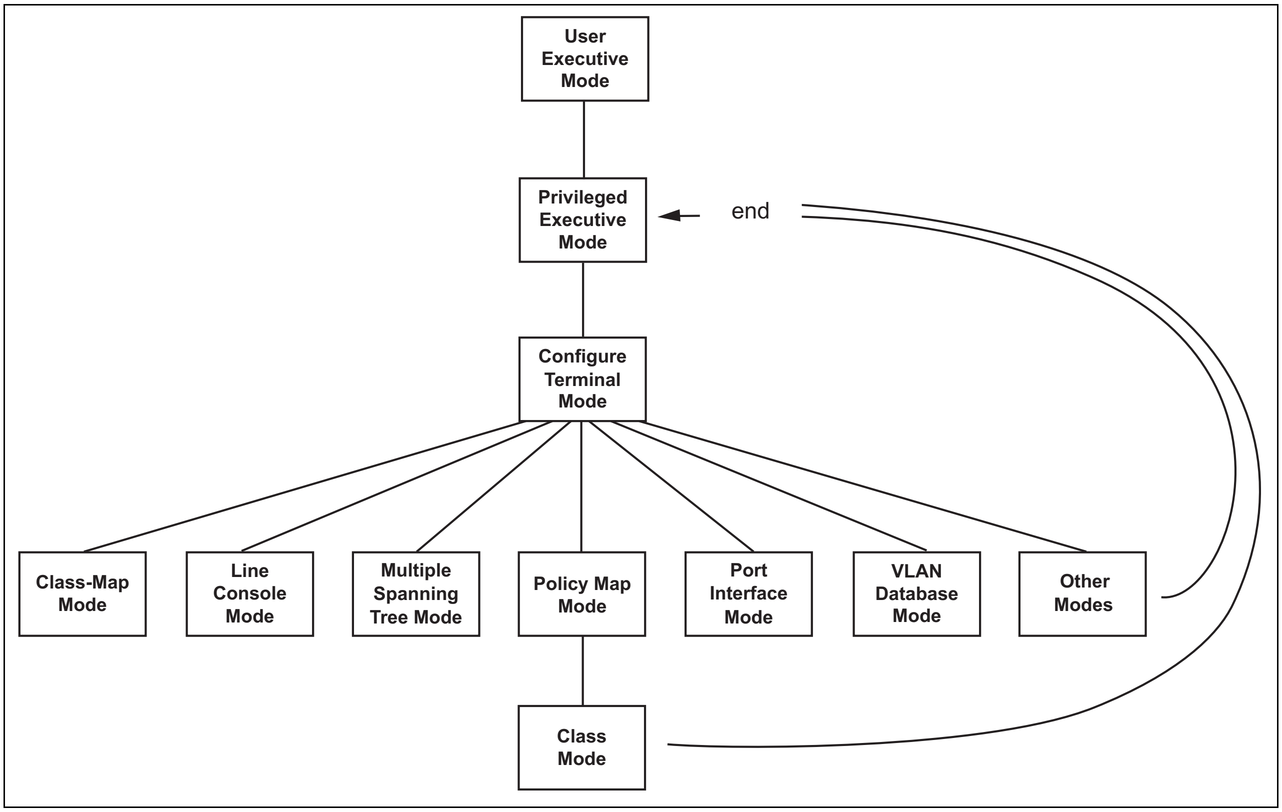


Figure 25. Returning to the Privileged Exec Mode with the END Command

Manager and Operator Accounts

The AlliedWare Plus interface has a manager access level and an operator access level. When you log on as a manager, you are given access to all the modes in the AlliedWare Plus Interface and have full control over the unit. When you log on as an operator, you are restricted to the User Exec mode from where you can view parameter settings and ping other devices.

Port Numbers in Commands

Port numbers are identified the same way in both command line interfaces.

Stand-alone AT-9400 Switches

To identify ports on stand-alone switches, simply enter the port numbers. If the command supports it, you can specify more than one port. The ports can be entered individually, as a range or both. The numbers of a range are separated with a dash, and the individual ports and ranges are separated with commas.

This example of the SET SWITCH PORT command from the standard command line interface activates ports 4 and 12

```
set switch port=4,12 status=enabled
```

This command, also from the standard command line interface, displays the statistics for ports 2 to 7, 19 and 22

```
show switch port=2-7,19,22 counter
```

This example of the INTERFACE command from the AlliedWare Plus interface lets you enter the Interface mode for ports 12 and 22 to 24 from where you can configure their settings:

```
interface 12,22-24
```

Though it’s not necessary, you can include the word “port” before a port number in the AlliedWare Plus commands. When specifying more than one port, include the word before just the first number. Here is how the previous command looks with the word “port”:

```
interface port12,22-24
```

AT-9400Ts Stacks

To identify the ports on the switches in an AT-9400Ts Stack, include the ID numbers of the switches as prefixes to the port numbers. (Refer to “SHOW STACK” on page 106 to view the module ID numbers of the switches in a stack.) Here is the format:

module ID.port number

This example enables port 15 and 21 on the switch with the module ID 1:

```
set switch port=1.15,1.21 status=enabled
```

To specify a range in a stack, include the module ID number with both the starting and ending numbers. For example

show switch port=4.12-4.16

Ranges can span switches. For example:

show switch port=1.1-2.24

Here’s another example using the AlliedWare Plus INTERFACE command:

```
interface 2.15-3.11
```

Note
All the command examples in this guide assume a stand-alone switch. If you are configuring ports on an AT-9400Ts Stack, remember to include the module ID numbers with the port numbers.

Formatting Commands

The standard command line interface and the AlliedWare Plus command line interface follow the same formatting conventions. In the case of the AlliedWare Plus command line interface, these conventions apply to 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 “sh” and then pressing the Tab key enters “show” 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.
- [ ] - Brackets indicate optional parameters.
- | - Vertical line separates parameter options for you to choose from.

Command Line Syntax Conventions

The following table describes the conventions used in the command interfaces.

Table 2. 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
WORD	Indicates a string of alphanumeric characters.	Switch_28_bldg_11
IFNAME or IF_NAME	Indicates a port number.	22,23
mask	Indicates a subnet mask.	255.255.255.0

Chapter 2

Basic Command Line Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

CLEAR SCREEN

AlliedWare Plus Command Available

Syntax

```
clear screen
```

Parameters

None.

Description

This command clears the screen.

Example

The following command clears the screen:

```
clear screen
```

AlliedWare Plus Command

Syntax

```
clear screen
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# clear screen
```

EXIT

AlliedWare Plus Command Available

Syntax

```
exit
```

Parameters

None.

Description

This command ends a management session. If you are managing a slave switch in an enhanced stack, the command returns you to the master switch from where you started the management session.

Example

The following command ends the current management session:

```
exit
```

Equivalent Commands

```
logoff
```

logout

quit

For information, see “LOGOFF, LOGOUT and QUIT” on page 57.

AlliedWare Plus Command

Syntax

```
quit
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# quit
```

HELP

AlliedWare Plus Command Available

Syntax

```
help
```

Parameters

None.

Description

This command displays a list of the CLI keywords with a brief description for each keyword.

Example

The following command displays the CLI keywords:

```
help
```

AlliedWare Plus Command

Syntax

```
?
```

Mode

All modes

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# ?
```

LOGOFF, LOGOUT and QUIT

AlliedWare Plus Command Available

Syntax

```
logoff
```

```
logout
```

```
quit
```

Parameters

None.

Description

These commands all perform the same function. They end a management session. If you are managing a slave switch in an enhanced stack, the commands return you to the master switch.

Example

The following command ends a management session:

```
logoff
```

AlliedWare Plus Command

Syntax

```
quit
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# quit
```

MENU

Syntax

```
menu
```

Parameters

None.

Description

This command displays the AT-S63 Main Menu. For instructions on how to use the menus, refer to the *AT-S63 Management Software Menus Interface User's Guide*.

Example

The following command displays the AT-S63 Main Menu:

```
menu
```

SAVE CONFIGURATION

AlliedWare Plus
Command
Available

Syntax

```
save configuration
```

Parameters

None.

Description

This command is used to store the switch’s current configuration in the active boot configuration file for permanent storage. When you enter the command, the switch copies its entire configuration into the file as a series of commands.

> **Note**
> You should always enter this command after changing the parameter settings of a switch because changes that are not saved are discarded when the switch is reset or powered off.

To view the name of the currently active boot configuration file, see “SHOW CONFIG” on page 270. To view the contents of a configuration file, see “SHOW FILE” on page 272.

Example

The following command saves your configuration changes to the active boot configuration file:

```
save configuration
```

AlliedWare Plus Command

Syntax

```
write
```

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

Mode

Privileged Exec mode

Description

These commands are equivalent to the SAVE CONFIGURATION command. Entering either of the commands prompts the switch to update its active configuration file with its current configuration.

Examples

```
awplus# write
```

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

SET PROMPT

Syntax

```
set prompt="prompt"
```

Parameter

prompt	Specifies the command line prompt. The prompt can be from one to 12 alphanumeric characters. Spaces and special characters are allowed. The prompt must be enclosed in quotes.

Description

This command changes the command prompt. Assigning each switch a different command prompt can make it easier for you to identify the different switches in your network when you manage them.

Note
If you define the system name before you set up a system prompt, the switch uses the first 16 characters of the system name as the prompt. See “SET SYSTEM” on page 85.

Example

The following command changes the command prompt to “Sales Switch”:

```
set prompt="Sales Switch"
```

Equivalent Command

```
set asyn prompt=”prompt”
```

For information, see “SET ASYN” on page 79.

SET SWITCH CONSOLEMODE

Syntax

```
set switch consolemode=menu|cli|awplus
```

Parameter

consolemode — Specifies the default management interface of your management sessions. Options are:

- menu — Specifies the menus interface.
- cli — Specifies the standard command line interface. This is the default value.
- awplus — Specifies the AlliedWare Plus command line interface.

Description

You use this command to specify the default management interface of your management sessions. All future management sessions will start with the designated management interface.

Example

The following command designates the menus interface as the default management interface:

```
set switch consolemode=menu
```

SHOW USER

Syntax

```
show user
```

Parameter

None.

Description

Displays the user account you used to log on to manage the switch.

Example

```
show user
```

Chapter 3

Basic Switch Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	Yes*
AT-9424T/GB	Yes*
AT-9424T/SP	Yes*
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

(*The Layer 2+ switches do not support the AlliedWare Plus commands or the standard AWPLUS command.)

This chapter contains the following commands:

AWPLUS

Syntax

```
awplus
```

Parameters

None.

Description

This command is used to start the AlliedWare Plus command line management session. When you enter the command, the management software displays the prompt for the User Exec mode in Figure 26.

```
AlliedWare Plus (TM) AT-9448T/SP AT-S63

awplus>
```

Figure 26. AlliedWare Plus Command Prompt - User Exec Mode

To enter the Privileged Exec mode, enter the ENABLE command, as shown in Figure 27.

```
AlliedWare Plus (TM) AT-9448T/SP AT-S63

awplus> enable
awplus#
```

Figure 27. AlliedWare Plus Command Prompt - Privileged Exec Mode

Note
This command and the AlliedWare Plus command interface are not supported on the Layer 2+ AT-9408LC/SP, AT-9424T/GB and AT-9424T/SP Switches.

Example

```
# awplus
```

DISABLE TELNET

AlliedWare Plus
Command
Available

Syntax

```
disable telnet
```

Parameters

None.

Description

This command disables the Telnet server on the switch. You might disable the server to prevent anyone from managing the switch with the Telnet application protocol or in the event you decide to use the Secure Shell protocol for remote management. The default setting for the Telnet server is enabled.

Example

The following command deactivates the Telnet server:

```
disable telnet
```

AlliedWare Plus Command

Syntax

```
no service telnet
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

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

ENABLE TELNET

AlliedWare Plus
Command
Available

Syntax

```
enable telnet
```

Parameters

None.

Description

This command activates the Telnet server on the switch. When the server is active, you can use a Telnet client to remotely manage the switch. To disable the server, refer to “DISABLE TELNET” on page 67. The default setting for the Telnet server is enabled.

Example

The following command activates the Telnet server:

```
enable telnet
```

AlliedWare Plus Command

Syntax

```
service telnet
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

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

PING

AlliedWare Plus Command Available

Syntax

```
ping ipaddress
```

Parameter

ipaddress	Specifies the IP address of an end node to be pinged.

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.

> **Note**
> The switch can only ping a device if there is a routing interface on the local subnet leading to the device. The switch uses the IP address of the interface as its source address. For instructions on how to add a routing interface to the switch, refer to "ADD IP INTERFACE" on page 708.

Example

The following command pings an end node with the IP address of 149.245.22.22

```
ping 149.245.22.22
```

The results of the ping are displayed on the screen.

AlliedWare Plus Command

Syntax

```
ping ipaddress
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> ping 149.122.14.15
```

RESET SWITCH

Syntax

```
reset switch
```

Parameters

None.

Description

This command does the following:

- ❐ Performs a soft reset on all ports. The reset takes less than a second to complete. The ports retain their current operating parameter settings. To perform this function on a per-port basis, refer to “RESET SWITCH PORT” on page 161.
- ❐ Resets the statistics counters for all ports to zero. To perform this function on a per-port basis, refer to “RESET SWITCH PORT COUNTER” on page 186.
- ❐ Deletes all dynamic MAC addresses from the MAC address table. To perform this function on a per-port basis, refer to “RESET SWITCH FDB” on page 197.

Example

This command resets the switch according to the description above:

```
reset switch
```

RESET SYSTEM

AlliedWare Plus Command Available

Syntax

```
reset system [name] [contact] [location]
```

Parameters

name Deletes the switch's name.

contact Deletes the switch's contact.

location Deletes the switch's location.

Description

This command is used to delete the switch's name, the name of the network administrator responsible for managing the unit, and the location of the unit. To set these parameters, refer to "SET SYSTEM" on page 85. To view the current settings, refer to "SHOW SYSTEM" on page 99.

Examples

This command deletes all three parameter settings:

```
reset system
```

This command deletes just the name:

```
reset system name
```

AlliedWare Plus Command

Syntax

```
no hostname
```

Mode

Configure mode

Description

You use this command to delete the switch's name. You cannot delete the contact or the location from the AlliedWare Plus command interface.

Example

This example deletes the current name of the switch without assigning a new value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no hostname
```

RESTART REBOOT

AlliedWare Plus Command Available

Syntax

```
restart reboot
```

Parameters

None.

Description

You use this command to reset stand-alone switches and stacks. You might reset a unit if it is experiencing a problem. The reset takes from twenty seconds to two minutes.

> **Note**
> Switches and stacks do not forward traffic while they are resetting. Some network traffic may be lost.

> **Note**
> Be sure to save your changes to active boot configuration file before resetting a switch or stack. Any unsaved changes will be lost.

Your local or remote management session ends when you reset a unit. To continue the management session, you must reestablish it.

To reset individual switches in a stack, refer to “RESTART SWITCH” on page 75.

Example

The following resets a switch or stack:

```
restart reboot
```

AlliedWare Plus Command

Syntax

```
system reboot
```

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# system reboot
```

RESTART SWITCH

AlliedWare Plus Command Available

Syntax 1

```
restart switch
```

Syntax 2

```
restart switch module=value|all
```

Syntax 3

```
restart switch config=none
```

Syntax 4

```
restart switch config=filename.cfg
```

Parameters

config — Specifies one of the following:

- none — Restores the default settings on a stand-alone switch or a stack.
- *filename*.cfg — Specifies the filename of a new active configuration file for a stand-alone switch or a stack. The file must already exist in the file system of a switch. If the filename contains spaces, enclose it in double quotes.

module — Specifies the stack ID number of a switch to reset in a stack. To reset all of the switches, use the ALL option. The ALL option is equivalent to the RESTART SWITCH command in Syntax 1.

Syntax 1 Description

You use this command to reset all of the switches in a stack. The devices initialize their management software and perform the discovery process. Afterwards, the master switch uses its configuration file to configure the parameter settings. The entire process may take several minutes.

Caution
A stack does not forward network traffic during the reset process. Some network traffic may be lost.

To reset a stand-alone switch, refer to “RESTART REBOOT” on page 73.

Syntax 2 Description

You use this command to reset individual switches in a stack. You can reset more than one switch at a time. When you reset a member switch, the remaining switches of a stack immediately perform the discovery process and resume forwarding traffic after the master switch configures the parameter settings. After a reset member switch has initialized its management software, a stack again performs the discovery process. The entire process may take several minutes.

To reset all of the switches, use the ALL option. This is equivalent to Syntax 1.

Note
A stack does not forward network traffic during the reset process. Some network traffic may be lost.

Syntax 3 Description

You use this command to restore the parameter settings on stand-alone switches and stacks to the default values. Before using this command, review the following:

❒ This command deletes all the routing interfaces as well as all the port-based and tagged VLANs.

❒ Restoring the default settings does not delete the files in a switch’s file system or the encryption keys in the key database. To delete these files, refer to “DELETE FILE” on page 260 and “DESTROY ENCO KEY” on page 850.

❒ Restoring the default settings does not change the settings in the active boot configuration file. To return the active configuration file to the default settings, you must use the SAVE CONFIGURATION command after the switch or stack reboots and you have reestablished your management session. Otherwise, the switch or stack reverts to the previous configuration the next time you reset it.

Note
This command resets a stand-alone switch or a stack. Network traffic is not forwarded during the reset process. Some network traffic may be lost.

For the list of the default values, refer to the *AT-S63 Management Software Features Guide*.

Syntax 4 Description

You use this command to configure a stand-alone switch or a stack with a different configuration file. You might do this to test the switch or stack with a different configuration.

When you enter the command, the switch or stack automatically resets itself and afterwards configures its parameters according to the settings in the specified configuration file. However, the assignment of the active boot configuration file does not change. Resetting or power cycling the switch again causes the unit to revert to its previous configuration. To change the assignment of the active boot configuration file, refer to "SET CONFIG" on page 266.

Your local or remote management session with the switch ends when you reset the switch. You must reestablish the session to continue managing the switch.

Syntax 1 Example

This command resets a stack:

```
restart switch
```

Syntax 2 Examples

This command resets a member switch with a stack ID 3 in a stack:

```
restart switch module=3
```

This command resets the member switches with the stack IDs 4 and 5:

```
restart switch module=4,5
```

Syntax 3 Example

This command restores the parameter settings to their default values on a stand-alone switch or a stack:

```
restart switch config=none
```

Syntax 4 Examples

This command uses a configuration file with the name "switch12a.cfg" to configure the parameter settings on a stand-alone switch:

```
restart switch config=switch12a.cfg
```

This command uses a configuration file with the name "stack_bld5.cfg" to configure the parameter settings on a stack:

```
restart switch config=stack_bld.cfg
```

Equivalent Command

```
restart reboot
```

For information, see “RESTART REBOOT” on page 73.

AlliedWare Plus Command

Syntax

```
system factory-reset
```

```
erase startup-config
```

Mode

Privileged Exec mode

Description

Both of these commands perform the same function. Analogous to Syntax 3 in the standard command, they are used to restore the default settings on stand-alone switches and stacks.

Unlike the standard command, these commands display a confirmation prompt. To restore the default settings, enter “Y” for yes at the prompt. Otherwise, enter “N” for no to cancel the procedure.

As explained in the standard command, restoring the default settings does not alter the settings in the active configuration file. To return the file to the default settings, you must save the configuration after the switch or stack resets. Otherwise, the switch or stack returns to its previous configuration the next time it is reset or power cycled.

Note
These commands cause a stand-alone switch or a stack to reset. Network traffic is not forwarded during the reset process. Some network traffic may be lost.

To reboot a stand-alone switch or a stack from the AlliedWare Plus command interface, refer to the AlliedWare Plus command in “RESTART REBOOT” on page 73.

Example

This command restores the parameters on a switch or a stack to their default values:

```
awplus> enable
awplus# system factory-reset
```

SET ASYN

AlliedWare Plus Command Available

Syntax

```
set asyn [speed=1200|2400|4800|9600|19200|38400|
57600|115200] [prompt=”prompt”]
```

Parameters

speed	Sets the speed (baud rate) of the serial terminal port on the switch. The default is 9600 bps.
prompt	Specifies the command line prompt. The prompt can be from one to 12 alphanumeric characters. Spaces and special characters are allowed. The prompt must be enclosed in double quotes. This parameter performs the same function as “SET PROMPT” on page 61.

Description

This command sets the baud rate of the serial terminal port on the switch. The port is used for local management of the switch. You can also use this command to set the command line prompt.

Note
A change to the baud rate of the port ends your management session if you are managing the switch locally. To reestablish a local management session you must change the speed of the terminal or the terminal emulator program to match the new speed of the serial terminal port on the switch.

Example

The following command sets the baud rate to 115200 bps:

```
set asyn speed=115200
```

Equivalent Command

```
set prompt="prompt"
```

For information, see “SET PROMPT” on page 61.

AlliedWare Plus Command

Syntax

```
baud-rate 1200|2400|4800|9600|19200|38400|57600|115200
```

Mode

Line Console mode

Description

You can use this command to set the speed of the terminal port, but not the command line prompt.

Example

This example sets the baud rate on the terminal port on the switch to 57600 bps:

```
awplus> enable
awplus# configure terminal
awplus(config-conf)# line console 0
awplus(config-line)# baud-rate 57600
```

SET DATE

AlliedWare Plus Command Available

Syntax

```
set date=dd-mm-yyyy
```

Parameter

date	Specifies the date for the switch in day-month-year format.

Description

You use this command to manually set the date on the switch if you are not using an SNTP server. The switch maintains the date even when the unit is powered off or reset.

Example

This command sets the switch’s date to December 11, 2004:

```
set date=11-12-2004
```

AlliedWare Plus Command

Syntax

```
clock set hh:mm:ss dd-mm-yyyy
```

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is used to manually set both the date and the time. The command must include both the date and the time.

Example

This example sets the time to 2:15 pm and the date to February 4, 2009:

```
awplus> enable
awplus# clock set 14:15:0 4-2-2009
```

SET PASSWORD MANAGER

Syntax

```
set password manager
```

Parameters

None.

Description

This command sets the manager’s password. The manager account allows you to view and change all switch parameters. The default password is “friend.” The password can be from 0 to 16 alphanumeric characters. Allied Telesis recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

Example

The following command changes the manager’s password:

```
set password manager
```

Follow the prompts to enter the new password.

Equivalent Command

```
set user manager password=password
```

For information, see “SET USER PASSWORD” on page 90.

SET PASSWORD OPERATOR

Syntax

```
set password operator
```

Parameters

None.

Description

This command sets the operator’s password. Logging in as operator allows you to only view the switch parameters. The default password is “operator.” The password can be from 0 to 16 alphanumeric characters. Allied Telesis recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

Example

The following command changes the operator’s password:

```
set password operator
```

Follow the prompts to enter the new password.

Equivalent Command

```
set user operator password=password
```

For information, see “SET USER PASSWORD” on page 90.

SET SWITCH CONSOLETIMER

AlliedWare Plus
Command
Available

Syntax

```
set switch consoletimer=value
```

Parameter

consoletimer Specifies the console timer in minutes. The range is 1 to 60 minutes. The default is 10 minutes.

Description

This command sets the console timer, which is used by the management software to end inactive management sessions. The AT-S63 Management Software automatically ends a session if it does not detect any management activity for the duration of the console timer. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch. To view the current console timer setting, refer to “SHOW SWITCH MODULE” on page 96.

Example

The following command sets the console timer to 25 minutes:

```
set switch consoletimer=25
```

AlliedWare Plus Command

Syntax

```
exec-timeout value
```

Mode

Line Console mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example sets the console timer to 15 minutes:

```
awplus> enable
awplus# configure terminal
awplus(config)# line console 0
awplus(config-line)# exec-timeout 15
```

SET SYSTEM

AlliedWare Plus
Command
Available

Syntax

```
set system [name="name"] [contact="contact"]
[location="location"] [maxmanager=value]
```

Parameters

name Specifies the name of the switch. The name can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes (“ “). Spaces are allowed.

contact Specifies the name of the network administrator responsible for managing the switch. The contact can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes. Spaces are allowed.

location Specifies the location of the switch. The location can be from 1 to 39 alphanumeric characters in length and must be enclosed in double quotes. Spaces are allowed.

maxmanager Specifies the maximum number of manager sessions that are allowed on the switch at the same time. The range is 1 to 3. The default is 1.

Description

This command is used to set a switch’s name, the name of the network administrator responsible for managing the unit, and the location of the unit.

This command is also used to set the maximum number of managers that can access the unit simultaneously. This feature makes it possible for more than one person to manage the unit at one time. The range is one to three manager sessions, with the default one manager session. This parameter does not affect operator sessions.

If a parameter already has a value, the new value replaces the existing value. To view the current values for these parameters, refer to “SHOW SYSTEM” on page 99. To delete a value without assigning a new value, refer to “RESET SYSTEM” on page 71.

Note
If you define the system name before you set up a system prompt, the switch uses the first 16 characters of the system name as the prompt. See “SET PROMPT” on page 61.

Examples

The following command sets a switch’s information:

```
set system name="Sales" contact="Jane Smith" location="Bldg
3, rm 212"
```

The following command sets just the system’s name:

```
set system name="PR Office"
```

This command sets the maximum number of manager sessions to two:

```
set system maxmanager=2
```

AlliedWare Plus Command

Syntax

To set the switch or stack’s name:

```
hostname name
```

To set the maximum number of management sessions permitted on the switch:

```
service terminal-length value
```

Mode

Configure mode

Description

The HOSTNAME command is used to assign a name to a switch. The name cannot contain spaces.

The AlliedWare Plus management interface does not have commands for setting the contact or the location. To set either of these parameters, use another management interface, like the standard command line interface.

The SERVICE TERMINAL-LENGTH command is equivalent to the MAXMANAGER parameter in the SET SYSTEM command and is used to set the maximum number of manager sessions that can be open on the switch simultaneously. The range is 1 to 3.

Examples

This example assigns the name “Switch12” to the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# hostname Switch12
```

This example deletes the current name without assigning a new value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no hostname
```

This example sets the maximum number of manager sessions to two:

```
awplus> enable
awplus# configure terminal
awplus(config)# service terminal-length 2
```

This example returns the maximum number of manager sessions to the default setting of one:

```
awplus> enable
awplus# configure terminal
awplus(config)# no service terminal-length
```

SET TELNET INSERTNULL

Syntax

```
set telnet insertnull=on|off
```

Parameters

insertnull Controls whether a NULL character is inserted after each CR sent by the Telnet server to the remote client. Options are:

on Sends a NULL character after each CR sent to the remote client.

off Specifies that no NULL character is sent to the remote client. This is the default setting.

Description

You use this command to toggle the Telnet server on the switch to add a NULL character after each CR for those Telnet clients that require the character in order to display the information correctly. The default setting on the switch is to not send the NULL character after a CR. To view the current setting, see “SHOW SWITCH MODULE” on page 96.

Example

This command configures the switch to send a NULL character after each CR during a Telnet management session:

```
set telnet insertnull=on
```

SET TIME

AlliedWare Plus
Command
Available

Syntax

```
set time=hh:mm:ss
```

Parameter

time	Specifies the hour, minute, and second for the switch’s time in 24-hour format.

Description

This command is used to set the time on the switch if you are using an SNTP server. With its onboard battery, the AT-9400 Switch can maintain the time even when the unit is powered off or reset.

Example

The following command sets the switch’s time to 4:34 pm and 52 seconds:

```
set time=16:34:52
```

AlliedWare Plus Command

The AlliedWare Plus command for setting the time is also the command for setting the date. For information, refer to the AlliedWare Plus command in “SET DATE” on page 81.

SET USER PASSWORD

Syntax

```
set user manager|operator password=password
```

Parameter

password	Specifies the password.

Description

This command sets the manager or operator’s password. The default manager password is “friend.” The default operator password is “operator.” The password can be from 0 to 16 alphanumeric characters. Allied Telesis recommends that you avoid special characters, such as spaces, asterisks, or exclamation points because some web browsers do not accept them in passwords. The password is case sensitive.

Example

The following command sets the operator’s password to “newby”:

```
set user operator password=newby
```

Equivalent Commands

```
set password manager
```

For information, see “SET PASSWORD MANAGER” on page 82

```
set password operator
```

For information, see “SET PASSWORD OPERATOR” on page 83

SHOW ASYN

Syntax

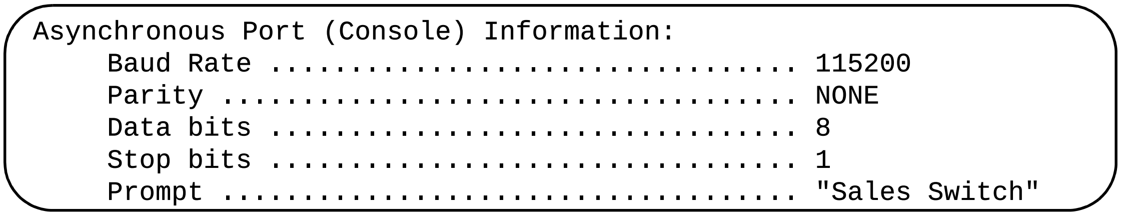
```
show asyn
```

Parameters

None.

Description

This command displays the settings for the serial terminal port on the switch, used for local management of the device. An example of the display is shown in Figure 28.



```
Asynchronous Port (Console) Information:
     Baud Rate ................................. 115200
     Parity .................................... NONE
     Data bits ................................. 8
     Stop bits ................................. 1
     Prompt .................................... "Sales Switch"
```

Figure 28. SHOW ASYN Command

To configure the serial port’s baud rate, refer to “SET ASYN” on page 79. To configure the command line prompt, refer to “SET PROMPT” on page 61. You cannot adjust the parity, data bits, or stop bit of the serial terminal port.

Example

The following command displays the serial terminal port settings:

```
show asyn
```

SHOW CONFIG DYNAMIC

Syntax

```
show config dynamic[=module]
```

Parameters

module Displays the settings of a specific switch module. You can specify only one module. For a list of modules, refer to Table 3.

Description

This command displays the settings of the switch parameters that have been changed from their default values, including those not yet saved to the active boot configuration file. The parameters are displayed in their command line command equivalents. You can view all of the settings or limit the display to just those of a particular switch module. An example of the display is shown in Figure 29.

```
---Start of current configuration ------------------

#
# System Configuration
#
set system name="Production Server"
set system contact="Jane Smith"
set system location="Bldg. 2, room 411"

#
# IP Configuration
#
```

Figure 29. SHOW CONFIG DYNAMIC Command

The MODULE variable is used to limit the display to the parameter settings of a particular switch module. You can specify only one module per command. The modules are listed in Table 3.

Table 3. Module Variable

Variable	Description
ACL	Port access control list
ARP	Static ARP entries
AUTH	Manager and operator passwords (encrypted) and RADIUS and TACACS+

Table 3. Module Variable (Continued)

Variable	Description
CLASSIFIER	Classifiers for ACL and QoS
DOS	Denial of service defense
ENCO	Encryption keys
ENHSTACK	Enhanced stacking
EVTLOG	Event log and syslog client
GARP	GARP and GVRP
IGMPSNOOP	IGMP snooping
INTF	Routing interfaces
LACP	Link Aggregation Control Protocol
MAC	Static MAC addresses
MACTIMER	MAC address table timeout value
MACVLAN	MAC address-based VLANs
MGMTACL	Management access control list
MIRROR	Source ports of port mirror
MIRTO	Destination port of port mirror
MLDSNOOP	MLD snooping
PKI	Public Key Infrastructure
PORT	Port configuration
PORTACC	802.1x port-based access control
PORTSEC	MAC address-based port security
PORTTRUNK	Static port trunks
QOS	Quality of Service
RIP	Routing Information Protocol
ROUTE	Static routes
RRPSNOOP	RRP snooping
SNMP	SNMP
SNTP	SNTP
SSH	Secure Shell protocol

Table 3. Module Variable (Continued)

Variable	Description
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SWITCH	Switch console timer, console startup mode, serial port baud rate, Telnet server
SYSTEM	Administrator name, switch name, and switch location
VLAN	Port-based and tagged VLANs, and multiple VLAN modes
WEBSERV	Web server

Examples

The following command displays all the switch parameter settings that have been changed from their default values:

```
show config dynamic
```

The following command displays the non-default parameter settings for IGMP snooping:

```
show config dynamic=igmpsnoop
```

SHOW CONFIG INFO

AlliedWare Plus Command Available

Syntax

```
show config info
```

Parameters

None.

Description

This command displays the settings of all the switch parameters, including those not yet saved to the active boot configuration file.

Example

The following command displays all the parameter settings on the switch:

```
show config info
```

AlliedWare Plus Command

Syntax

```
show running-config
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

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

SHOW SWITCH MODULE

Syntax

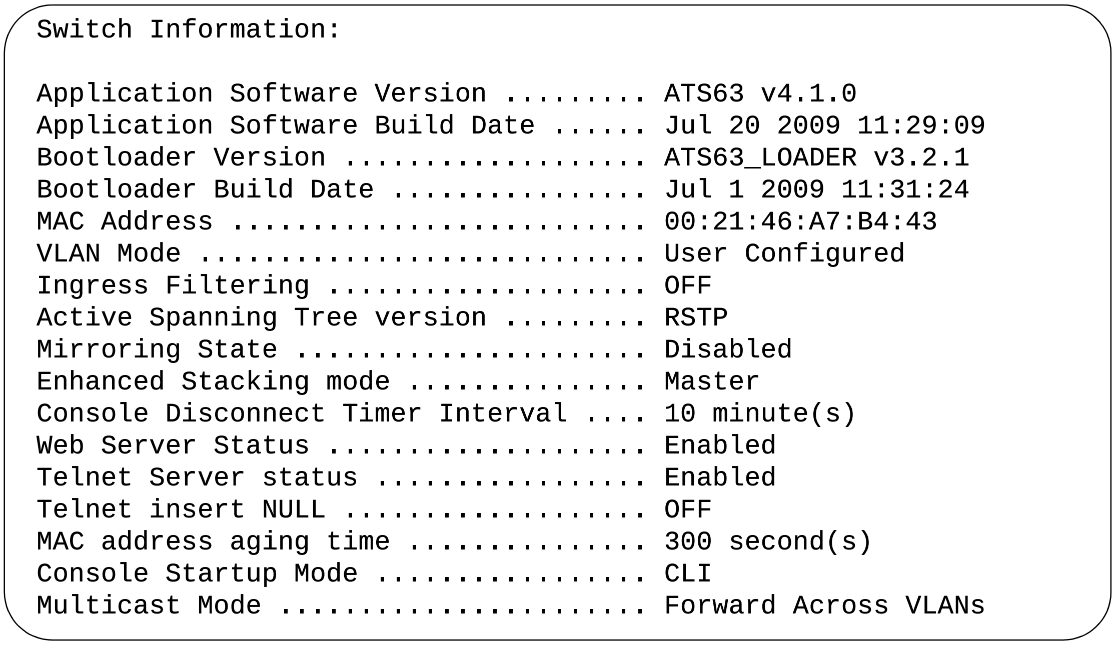
```
show switch module=1
```

Parameters

None.

Description

This command displays the same information for stand-alone switches and AT-9400Ts Stacks. An example of the display is shown in Figure 30.



```
Switch Information:

Application Software Version ......... ATS63 v4.1.0
Application Software Build Date ...... Jul 20 2009 11:29:09
Bootloader Version ................... ATS63_LOADER v3.2.1
Bootloader Build Date ................ Jul 1 2009 11:31:24
MAC Address .......................... 00:21:46:A7:B4:43
VLAN Mode ............................ User Configured
Ingress Filtering .................... OFF
Active Spanning Tree version ......... RSTP
Mirroring State ...................... Disabled
Enhanced Stacking mode ............... Master
Console Disconnect Timer Interval .... 10 minute(s)
Web Server Status .................... Enabled
Telnet Server status ................. Enabled
Telnet insert NULL ................... OFF
MAC address aging time ............... 300 second(s)
Console Startup Mode ................. CLI
Multicast Mode ....................... Forward Across VLANs
```

Figure 30. SHOW SWITCH MODULE Command

For an AT-9400Ts Stack the first five lines apply to just the master switch. The command accepts other module numbers, but it always displays the same information. To determine the version numbers and build dates of the AT-S63 Management Software on the member switches of a stack, refer to “SHOW SYSTEM VERSION” on page 101.

This command displays the following information:

- ❒ Application software version and Application software build date - The version number and build date of the AT-S63 Management Software.
- ❒ Bootloader version and Bootloader build date - The version number and build date of the AT-S63 bootloader.

- MAC address - The MAC address of the switch. This value cannot be changed.
- VLAN mode - The switch's VLAN mode. The three possible VLAN modes are:
  - User configured (for creating your own port-based and tagged VLANs)
  - 802.1Q-compliant
  - Non-802.1Q-compliant.

  The default is user configured. To set a switch's VLAN mode, refer to "SET SWITCH VLANMODE" on page 657.
- Ingress filtering - The status of ingress filtering on the switch. When ingress filtering is activated, tagged frames are filtered when they are received on a port. When ingress filtering is deactivated, which is the default, tagged frames are filtered before they are transmitted out a port. To set ingress filtering, refer to "SET SWITCH INFILTERING" on page 656.
- Active Spanning Tree version - The spanning tree protocol that has been designated as the active protocol on the switch. To configure or enable a spanning tree protocol, you must first designate it as the active protocol on the switch. The switch supports, STP, RSTP, and MSTP. The default is RSTP. To select an active spanning tree protocol, refer to "ACTIVATE STP" on page 574, "ACTIVATE RSTP" on page 590, and "ACTIVATE MSTP" on page 612.
- Mirroring state - The status of port mirroring. The display includes the destination port as well as the ingress and egress source ports if port mirroring is activated on the switch. To configure port mirroring, refer to "SET SWITCH MIRROR" on page 238 and "SET SWITCH PORT MIRROR" on page 239.
- Enhanced stacking mode - The enhanced stacking mode of the switch, which can be master, slave, or unavailable. The default is slave. To set the enhanced stacking status, refer to "SET SWITCH STACKMODE" on page 112.
- Console disconnect timer interval - The current value of the console timer, used by the management software to end inactive management sessions. The AT-S63 Management Software ends a local or remote management session if it does not detect any management activity for the duration of the console timer. The default is 10 minutes. To set the console timer, refer to "SET SWITCH CONSOLETIMER" on page 84.
- Web server status - The status of the web server. When the web server is disabled, you cannot remotely manage the switch using a web browser and the web browser interface. The default setting is enabled. To enable or disable the server, refer to "ENABLE HTTP SERVER" on page 837 and "DISABLE HTTP SERVER" on page 836.

- ❐ Telnet server status - The status of the Telnet server. When the Telnet server is disabled, you cannot remotely manage the switch using the Telnet application protocol. The default setting is enabled. To enable or disable the server, refer to “ENABLE TELNET” on page 68 and “DISABLE TELNET” on page 67.
- ❐ Telnet insert NULL - The status of the Telnet NULL parameter. When ON, the Telnet server on the switch adds a NULL character after each CR for those Telnet clients that require the character to display the information correctly. When OFF, the default setting, no NULL character is set after a CR. To set this feature, see “SET TELNET INSERTNULL” on page 88.
- ❐ MAC address aging time - The current value for the MAC address aging timer. The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. To set this value, refer to “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 198.
- ❐ Console startup mode - The management interface —menus or command line — that initially appears when you start a local or remote management session. The default is the command line interface. To set the startup mode, refer to “SET SWITCH CONSOLEMODE” on page 62.
- ❐ Multicast Mode - The multicast mode, which determines the behavior of the switch when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets To set the multicast mode, refer to “SET SWITCH MULTICASTMODE” on page 584.

Example

The following command displays the switch information described above:

```
show switch module=1
```

SHOW SYSTEM

AlliedWare Plus Command Available

Syntax

```
show system
```

Parameters

None.

Description

This command displays the following information:

- ❒ MAC Address: The MAC address of the switch.
- ❒ Model Name: The model name of the switch.
- ❒ Serial Number: The serial number of the switch.
- ❒ IP Address: The IP address of the local interface.
- ❒ Subnet Mask: The subnet mask of the local interface.
- ❒ System Up Time: The length of time since the switch was last reset or power cycled.
- ❒ Bootloader: The version number and build date of the AT-S63 bootloader.
- ❒ Application: The version number and build date of the AT-S63 Management Software.
- ❒ System Name: The name of the switch.
- ❒ Administrator: The name of the network administrator responsible for managing the switch.
- ❒ Location: The location of the switch, (for example, 4th Floor - rm 402B).

Note
To configure the name, administrator, and location parameters, refer to "SET SYSTEM" on page 85.

- ❒ Power Information: The status of the main power supply, the redundant power supply (if present), and internal power consumption.
- ❒ Temperature (Deg.C): The ambient temperature as measured where the air enters the cooling vents on the side of the unit.
- ❒ Fan Information: The speed or operating status of the system fan(s).

Example

The following command displays the above information about the switch:

```
show system
```

AlliedWare Plus Command

Syntax

```
show system
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show system
```

SHOW SYSTEM VERSION

Syntax

```
show system version module=id_number|all
```

Parameters

module Specifies the ID number of a switch in an AT-9400Ts Stack. You can specify more than one ID number at a time. To specify all of the switches in a stack, use the ALL option.

None.

Description

This command is used to display the version numbers of the AT-S63 Management Software on the master and member switches in an AT-9400Ts Stacks. To display this information on stand-alone switches, refer to “SHOW SWITCH MODULE” on page 96 or “SHOW SYSTEM” on page 99.

Examples

This command displays the version number of the AT-S63 Management Software on the master switch:

```
show system version module=1
```

This command displays the version numbers of the AT-S63 Management Software on the master switch and member switch 3:

```
show system version module=1,3
```

This command displays the version numbers of the management software on all of the switches in a stack:

```
show system version module=all
```

SHOW TIME

AlliedWare Plus
Command
Available

Syntax

```
show time
```

Parameters

None.

Description

This command shows the system’s current date and time.

Example

The following command shows the system’s date and time.

```
show time
```

AlliedWare Plus Command

Syntax

```
show clock
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show clock
```

Chapter 4
AT-9400Ts Stack Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	
AT-9424T/POE	
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

SET STACK

Syntax

```
set stack moduleid=value newmoduleid=auto|static|value
priority=value
```

Parameters

mymoduleid — Specifies the switch's current ID number. To view this number, refer to "SHOW STACK" on page 106.

newmoduleid — Specifies a new stack ID number for the switch. Options are:

- auto — Sets the switch for stand-alone operation. At this setting, the switch uses the BOOT.CFG file as its default configuration file.
- static — Converts the switch's current dynamic module ID into a static ID.
- *value* — Assigns a static module ID to the switch. The range is 1 to 8.

priority — Specifies a stack priority value for the switch, used with dynamic stack ID numbers. The range is 1 to 16. The lower the value the higher the priority. The default value is 16.

Description

This command assigns an ID number to a switch. ID numbers can be either dynamic or static. Dynamic ID numbers are based on the devices' MAC addresses or their priority values, and are assigned during the discovery process of the stack. Static ID numbers are numbers manually assigned to the devices.

Note the following before performing this command:

- ❒ This command should be performed before a switch is connected to a stack. The results may be unpredictable if you perform this command while a switch is part of a stack.
- ❒ You must reset or power cycle the unit after performing this command to activate a switch's new ID number.
- ❒ You do not have to issue the SAVE CONFIGURATION command with this command. A device's new ID number is automatically stored in a hidden system file in the unit's file system.

Note
All of the switches of a stack must have the same type of stack ID number of static or dynamic. A stack will not function if one or more of the module ID numbers are dynamic and others are static.

Examples

This command assigns the static ID 1 to the switch. The command assumes that the switch's current module ID number of 1 was set dynamically:

```
set stack moduleid=1 newmoduleid=1
```

This command assigns to the switch the static ID 4. The switch's current module ID number is 1:

```
set stack moduleid=1 newmoduleid=4
```

This command assigns the static ID 3 to the switch. The switch's current module ID number is 2:

```
set stack moduleid=2 newmoduleid=3
```

This command sets the switch's module ID number dynamically:

```
set stack moduleid=1 newmoduleid=auto
```

This command sets the switch's module ID number dynamically and assigns it a priority of 5:

```
set stack moduleid=1 newmoduleid=auto priority=5
```

SHOW STACK

AlliedWare Plus Command Available

Syntax

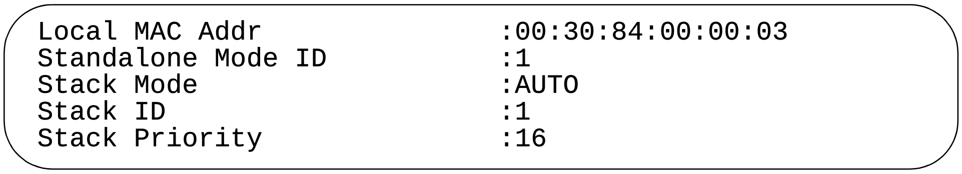
```
show stack
```

Parameters

None.

Description

This command displays the module ID number of a switch. The command displays different information depending on whether the switch is a stand-alone unit or the master switch of a functioning stack. Figure 31 is an example of the information from a stand-alone switch. This information is useful when setting or changing a switch’s ID number, which should only be performed when a switch is not connected to a stack.



```
Local MAC Addr              :00:30:84:00:00:03
Standalone Mode ID          :1
Stack Mode                  :AUTO
Stack ID                    :1
Stack Priority              :16
```

Figure 31. SHOW STACK Command of a Stand-alone Switch

The fields are defined here:

- Local MAC Addr: The MAC address of the switch.
- Standalone Mode ID: The ID number of the switch when the device is not a part of a stack. This parameter can be ignored.
- Stack Mode: The method by which the ID number was assigned. Auto means the number was assigned dynamically by the management software when the switch was powered on. Static means the number was assigned with the SET STACK command.
- Stack ID: The switch’s current module ID number.
- Stack Priority: The switch’s current stack priority value, used to control dynamic ID numbers.

Note
If you changed a switch’s ID number with the SET STACK command but do not see the change reflected in this command, it could be because you did not reset the switch. A change to a switch’s ID number does not take effect until the unit is reset.

Figure 32 is an example of the command from the master switch of a functioning stack. The switches in the stack and their module ID numbers are displayed in a table.

```
Local MAC Addr              :00:30:84:00:00:02
Master MAC Addr             :00:30:84:00:00:02
Backup Master MAC Addr      :00:30:84:00:00:54
Topology                    :Duplex_Chain
My ModuleID                 :1
ModuleID Assignment Mode    :STATIC
Current State               :Master
Module Count                :4

--------------------------------------------------------------
Module |  Stack State  |  Model Name   | Priority  | Mac Address
1      |  Master       |  AT-9424Ts/XP | 16        | 00:30:84:00:00:02
2      |  Member       |  AT-9424Ts/XP | 16        | 00:30:84:00:00:52
3      |  Member       |  AT-9424Ts/XP | 16        | 00:30:84:00:00:22
4      |  Member       |  AT-9424Ts/XP | 16        | 00:30:84:00:00:82
```

Figure 32. SHOW STACK Command of a Stack

The fields and columns are defined here:

- Local MAC Addr - The MAC address of the master switch of the stack. The local and master MAC addresses will always be the same.
- Master MAC Addr - The MAC address of the master switch of the stack.
- Backup Master MAC Addr - The MAC address of the backup master switch of the stack. A stack will have a backup master if the switches have static ID numbers. A stack with dynamic module ID numbers will not have a backup master.
- Topology - The cabling topology of the stack. Possible values are Duplex_Chain and Duplex_Ring.
- My ModuleID - The module ID number of the master switch of the stack. The master switch always has the ID number 1.
- ModuleID Assignment Mode - The assignment method of the ID numbers of the switches. If AUTOMATIC, the switches were assigned dynamic ID numbers. If STATIC, the switches were assigned static ID numbers.
- Current State - The current state of the master switch. This will always be Master.
- Module Count - The number of switches in the stack.
- Module - The module ID number of a switch.
- Stack State - The state of a switch. A switch will be either Master or Member.
- Model Name - The Allied Telesis model name of a switch.

- ❐ Priority - The priority number of a switch. The range is 1 to 16. The lower the number, the higher the priority. To set this value, refer to “SET STACK” on page 104. This value only applies when the ID numbers are set automatically.
- ❐ Mac Address - The MAC address of a switch.

Example

```
show stack
```

AlliedWare Plus Command

Syntax

```
show stack
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show stack
```

Chapter 5

Enhanced Stacking Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

ACCESS SWITCH

Syntax

```
access switch number=number|macaddress=macaddress
```

Parameters

number
: Specifies the number of the switch in an enhanced stack that you want to manage. You view this number using the SHOW REMOTELIST command.

macaddress
: Specifies the MAC address of the switch you want to manage. This can also be displayed using the SHOW REMOTELIST command. You can enter the address in either of the following formats:

xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

Description

This command starts a management session on another switch that supports enhanced stacking, such as another AT-9400 Switch or an AT-8500 Switch. You can specify the switch by switch number or by MAC address, both of which are displayed with “SHOW REMOTELIST” on page 114.

Note
You must perform the ACCESS SWITCH command from the management session of the master switch where you started the session. This command will not work from a management session of a slave switch. To determine the master or slave status of your switch, use “SHOW SWITCH MODULE” on page 96.

Note
You must perform the SHOW REMOTELIST command before the ACCESS SWITCH command.

When you are finished managing a slave switch, use the LOGOFF, LOGOUT, or QUIT command to end the management session and to return back to the master switch from where you started the management session. For information, refer to “LOGOFF, LOGOUT and QUIT” on page 57.

Examples

The following command starts a management session on switch number 12:

```
access switch number=12
```

The following command starts a management session on a switch with the MAC address 00:30:84:52:02:11

```
access switch macaddress=003084520211
```

SET SWITCH STACKMODE

Syntax

```
set switch stackmode=master|slave|unavailable
```

Parameter

stackmode — Specifies the enhanced stacking mode of the switch. The options are:

master	Specifies the switch’s stacking mode as master. A master switch must be assigned an IP address and subnet mask.
slave	Specifies the switch’s stacking mode as slave. A slave does not need an IP address. This is the default setting for a switch.
unavailable	Specifies the switch’s stacking mode as unavailable. A switch with this status cannot be managed from an enhanced stack. It can be managed locally through its RS-232 terminal port or remotely if it is assigned an IP address and subnet mask.

Description

This command sets a switch’s enhanced stacking status.

Note
To determine the master or slave status of a switch, use “SHOW SWITCH MODULE” on page 96.

Note
You cannot change the stacking status of a switch through enhanced stacking. If a switch does not have an IP address or subnet mask, such as a slave switch, you must use a local management session to change its stacking status. If the switch has an IP address and subnet mask, such as a master switch, you can use a local session or a remote Telnet or SSH management session to change its stacking status.

Example

The following command sets the switch’s stacking status to master:

```
set switch stackmode=master
```

SHOW REMOTELIST

Syntax

```
show remotelist [sorted by=macaddress|name]
```

Parameter

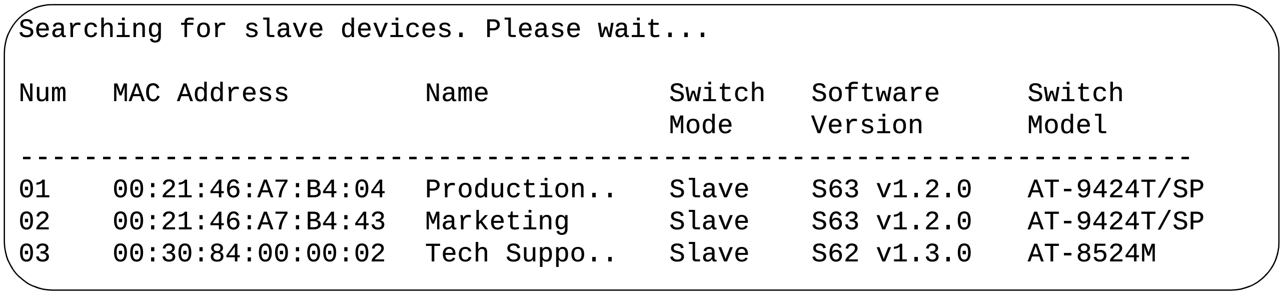
sorted Sorts the list either by MAC address or by name. The default is by MAC address.

Description

This command displays the list of switches in an enhanced stack. The list does not include the master switch where you started the management session or switches with a stacking status of unavailable.

> **Note**
> You must perform the SHOW REMOTELIST command from the management session of the master switch where you started the management session. This command will not work from a slave switch. Nor will the command work from a master switch that you accessed through enhanced stacking from another master switch. To determine the master or slave status of your switch, use “SHOW SWITCH MODULE” on page 96.

An example of the information displayed by this command is shown in Figure 33.



```
Searching for slave devices. Please wait...

Num   MAC Address         Name            Switch   Software      Switch
                                          Mode     Version       Model
------------------------------------------------------------------------
01    00:21:46:A7:B4:04   Production..    Slave    S63 v1.2.0    AT-9424T/SP
02    00:21:46:A7:B4:43   Marketing       Slave    S63 v1.2.0    AT-9424T/SP
03    00:30:84:00:00:02   Tech Suppo..    Slave    S62 v1.3.0    AT-8524M
```

Figure 33. SHOW REMOTELIST Command

Examples

The following command displays the switches in an enhanced stack, sorted by MAC address, the default sorting method:

```
show remotelist
```

The following command displays the switches sorted by name:

```
show remotelist sorted by=name
```

Chapter 6

Simple Network Time Protocol (SNTP) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

ADD SNTPSERVER PEER|IPADDRESS

AlliedWare Plus Command Available

Syntax

```
add sntpserver peer|ipaddress=ipaddress
```

Parameter

peer ***or*** ipaddress	Specifies the IP address of an SNTP server. These parameters are equivalent.

Description

This command adds the IP address of an SNTP or NTP server to the SNTP client on the switch. The switch uses the SNTP or NTP server to set its date and time. You can specify only one SNTP or NTP server.

Note
The switch must have a routing interface on the local subnet leading to the SNTP or NTP server. The switch uses the IP address of the interface as its source address to communicate with the server. For instructions on how to add a routing interface to the switch, refer to “ADD IP INTERFACE” on page 708.

If the routing interface obtains its IP address and subnet mask from a DHCP sever, you can configure the DHCP server to provide the switch with an IP address of an NTP or SNTP server. If you configured the DHCP server to provide this address, then you do not need to enter it with this command.

Example

The following command specifies the IP address of 148.35.16.248 for the SNTP server:

```
add sntpserver ipaddress=148.35.16.248
```

AlliedWare Plus Command

Syntax

```
ntp server ipaddress
```

Mode

Configure mode

Description

This command is used to identify the IP address of a SNTP server. The SNTP client is automatically activated after you enter this command. With the other management interfaces you have to use different commands to define the IP address of the server and to activate the client.

Example

This example defines the IP address of the SNTP server as 148.77.122.54 and activates the client:

```
awplus> enable
awplus# configure terminal
awplus(config)# ntp server 148.77.122.54
```

DELETE SNTPSERVER PEER|IPADDRESS

AlliedWare Plus
Command
Available

Syntax

```
delete sntpserver peer|ipaddress=ipaddress
```

Parameter

peer ***or*** ipaddress — Specifies the IP address of an SNTP server. The parameters are equivalent.

Description

This command deletes the IP address of the SNTP server from the SNTP client software on the switch and returns the parameter to the default value of 0.0.0.0. To view the IP address, refer to “SHOW SNTP” on page 126.

Example

The following command deletes the SNTP server with the IP address 148.35.16.248:

```
delete sntpserver ipaddress=148.35.16.248
```

AlliedWare Plus Command

Syntax

```
no ntp server ipaddress
```

Mode

Configure Terminal

Description

This command automatically deactivates the SNTP client when you remove from the client the IP address of the SNTP server. The other management interfaces have different commands for removing the IP address of the server and for deactivating the client.

Example

This example removes the IP address of the SNTP server and deactivates the client:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ntp server 152.140.22.4
```

DISABLE SNTP

AlliedWare Plus
Command
Available

Syntax

```
disable sntp
```

Parameters

None.

Description

This command is used to disable the SNTP client. The default setting for the SNTP client is disabled.

Example

The following command disables the SNTP client:

```
disable sntp
```

AlliedWare Plus Command

To disable the SNTP client from the AlliedWare Plus commands, refer to the AlliedWare Plus command in “DELETE SNTPSERVER PEER|IPADDRESS” on page 120.

ENABLE SNTP

AlliedWare Plus Command Available

Syntax

```
enable sntp
```

Parameters

None.

Description

This command is used to enable the SNTP client. When the SNTP client is enabled, the switch or stack obtains its date and time from an SNTP server whenever the unit is powered on or reset. To specify the IP address of an NTP server, refer to “ADD SNTPSERVER PEER|IPADDRESS” on page 118. The default setting for the SNTP client is disabled.

Example

The following command enables the SNTP client:

```
enable sntp
```

AlliedWare Plus Command

To enable the SNTP client from the AlliedWare Plus commands, refer to the AlliedWare Plus command in “ADD SNTPSERVER PEER|IPADDRESS” on page 118.

PURGE SNTP

Syntax

```
purge sntp
```

Parameters

None.

Description

This command clears the SNTP configuration and disables the SNTP client. To disable the SNTP client and retain the configuration, see “DISABLE SNTP” on page 121.

Example

The following command clears the SNTP configuration and disables the client:

```
purge sntp
```

SET SNTP

AlliedWare Plus Command Available

Syntax

```
set sntp [dst=enabled|disabled] [pollinterval=value]
[utcoffset=value]
```

Parameters

dst	Enables or disables daylight savings time.
pollinterval	Specifies the time interval between two successive queries by the STNP client on the switch to the SNTP server. The range is 60 to 1200 seconds. The default is 600 seconds.
utcoffset	Specifies the time difference in hours between UTC and local time. The range is -12 to +12 hours. The default is 0 hours.

Description

This command enables or disables daylight savings time and sets the polling and UTC offset times for the SNTP client software.

> **Note**
> The switch does not set the DST automatically. If the switch is in a locale that uses DST, you must remember to enable this in April when DST begins and disable it in October when DST ends. If the switch is in a locale that does not use DST, set this option to disabled all the time.

Example

The following command enables daylight savings time, sets the poll interval to 300 seconds, and sets the UTC offset to -8 hours:

```
set sntp dst=enabled pollinterval=300 utcoffset=-8
```

AlliedWare Plus Command

Syntax

To enable daylight savings time on the SNTP client:

```
clock summer-time
```

To disable daylight savings time:

```
no clock summer-time
```

To specify the time difference between UTC and local time, in the range -12 to +12 hours:

```
clock timezone plus|minus value
```

Mode

Configure Terminal

Description

This command is used to enable and disable DST, and to specify the time difference between UTC and local time. There is no AlliedWare Plus command for setting the polling interval of the STNP client.

Example

This command enables daylight savings time on the SNTP client:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock summer-time
```

This command disables daylight savings time:

```
awplus> enable
awplus# configure terminal
awplus(config)# no clock summer-time
```

This command specifies a time difference of -2 hours between UTC and local time:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock timezone minus 2
```

This command specifies a time difference of +4 hours between UTC and local time:

```
awplus> enable
awplus# configure terminal
awplus(config)# clock timezone plus 4
```

SHOW SNTP

AlliedWare Plus
Command
Available

Syntax

```
show sntp
```

Parameters

None.

Description

This command displays the current settings for the client SNTP software on the switch. An example of the display is shown in Figure 34.

```
SNTP Configuration:
   Status ........................ Disabled
   Server ........................ 0.0.0.0
   UTC Offset .................... +0
   Daylight Savings Time (DST) ... Enabled
   Poll Interval ................. 600 seconds
   Last Delta .................... +0 seconds
```

Figure 34. SHOW SNTP Command

The information displayed by this command is described here:

- Status - The status of the SNTP client software on the switch. The status can be either enabled or disabled. If enabled, the switch seeks its date and time from an SNTP server. The default is disabled.
- SNTP - The IP address of the SNTP server.
- UTC Offset - The time difference in hours between UTC and local time. The range is -12 to +12 hours. The default is 0 hours.
- Daylight Savings Time (DST) - The status of the daylight savings time setting. The status can be enabled or disabled.
- Poll interval - The time interval between two successive queries to the SNTP server. The range is 60 to 1200 seconds. The default is 600 seconds.
- Last Delta - The last adjustment applied to the system time. It is the drift in the system clock between two successive queries to the SNTP server.

Example

The following command displays SNTP client software information:

```
show sntp
```

AlliedWare Plus Command

Syntax

```
show ntp associations
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show ntp associations
```

SHOW TIME

AlliedWare Plus
Command
Available

Syntax

```
show time
```

Parameters

None.

Description

This command shows the system's current date and time.

Example

The following command shows the system's date and time.

```
show time
```

AlliedWare Plus Command

Syntax

```
show clock
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This command displays the switch's STP settings:

```
awplus# show clock
```

Chapter 7

SNMPv1 and SNMPv2c Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD SNMP COMMUNITY

AlliedWare Plus
Command
Available

Syntax

```
add snmp community="community" [traphost=ipaddress]
[manager=ipaddress]
```

Parameters

community Specifies an existing SNMP community string on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character such as an exclamation point. Otherwise, the quotes are optional.

traphost Specifies the IP address of a trap receiver.

manager Specifies the IP address of a management station to have SNMP access to the switch using the community string.

Description

This command adds the IP addresses of trap receivers and management stations to existing community strings.

The TRAPHOST parameter specifies a trap receiver for the SNMP community string. This is the IP address of a device to which traps generated by the switch are sent. A community string can have up to eight IP addresses of trap receivers, but only one can be added at a time with this command.

The MANAGER parameter specifies a management station to be allowed SNMP management access to the switch using the community string. This parameter applies only to community strings with a closed status. A community string can have up to eight IP addresses of management stations, but only one can be added at a time with this command.

To create a new community string, refer to “CREATE SNMP COMMUNITY” on page 133. To view the current community strings, refer to “SHOW SNMP” on page 148.

Examples

The following command permits access by a management station with the IP address 149.212.11.22 to the switch through the “private” community string:

```
add snmp community=private manager=149.212.11.22
```

The following command adds the IP address 149.212.10.11 as a trap receiver to the “public” community string:

```
add snmp community=public traphost=149.212.10.11
```

AlliedWare Plus Command

Syntax

```
snmp-server host ipaddress trap community_string|
informs community_string
```

Mode

Configure mode

Description

The IPADDRESS parameter specifies the IP address of a network node to be assigned as a trap receiver or a manager of a community string on the switch. If you want the node to be a trap receiver, use the TRAP parameter and specify a community string. If you want the node to be able to manage the switch, use the INFORMS parameter to specify the community string through which the node should access the switch. You use the INFORMS parameter only for strings that have a closed status.

You cannot specify both the TRAP parameter and the INFORMS parameter in the same command. If an IP address is to be both a trap receiver and a manager of a community string, you must enter this command twice.

Examples

This example assigns the IP address 149.44.12.44 as a trap receiver to the private community string:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 149.44.12.44 trap private
```

This example assigns the IP address 124.112.32.7 as a manager to the community string “mgr142a” which has a closed status. This enables the node of the IP address to manage the switch through the community string:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 124.112.32.7 informs
mgr142a
```

This example assigns the IP address 152.34.32.18 as both a trap receiver and a manager to the community string “tlpaac:”

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server host 152.34.32.18 trap tlpaac
awplus(config)# snmp-server host 152.34.32.18 informs tlpaac
```

CREATE SNMP COMMUNITY

AlliedWare Plus
Command
Available

Syntax

```
create snmp community="community" [access=read|write]
[open=yes|no|on|off|true|false] [traphost=ipaddress]
[manager=ipaddress]
```

Parameters

community — Specifies a new community string. The maximum length of a community string is 15 alphanumeric characters. Spaces are allowed. The name must be enclosed in double quotes if it includes a space or other special character such as an exclamation point. Otherwise, the quotes are optional. The string is case sensitive.

access — Specifies the access level of the new community string. Options are “read” for read only access and “write” for both read and write access. The default is “read.”

open — Specifies the open or closed status of the community string. The options are:

- yes, on, true — The community string is open, meaning any management station can use the string to access the switch. These values are equivalent.
- no, off, false — The community string is closed, meaning only those management stations whose IP addresses are assigned to the string can use it to access the switch. You can assign a management IP address to the string using the MANAGER option in this command. The default setting for a community string is closed. These values are equivalent.

traphost — Specifies the IP address of a trap receiver to receive system traps.

manager — Specifies the IP address of a management station that can use the community string to access the switch. This option applies if you specify the status of the community string as closed. A community string can have up to eight IP addresses of management stations, but only one can be assigned with this option.

Description

This command creates a new SNMP community string on the switch. The switch comes with two default community strings, “public,” with an access of read only, and “private,” with an access level of read and write. A switch can support up to eight community strings.

The COMMUNITY parameter specifies the new community string. The string can be up to 15 alphanumeric characters. The string is case sensitive.

The ACCESS parameter defines the access level for the new community string. The access level can be either read or read and write. The READ option specifies the read access level and the WRITE option specifies the read and write access level.

The OPEN parameters controls whether the string will have an open or closed status. If you specify YES, ON or TRUE, the string will have an open status. Any management station will be able to use the string to access the switch. If you specify NO, OFF or FALSE, the string will have a closed status and only those management stations whose IP addresses are assigned to the switch will be able to use the string. This is the default.

The TRAPHOST parameter specifies the IP address of a trap receiver to receive traps from the switch. A community string can have up to eight trap receivers, but only one can be assigned when a community string is created. To add IP addresses of trap receivers to an existing community string, see “ADD SNMP COMMUNITY” on page 130.

The MANAGER parameter specifies the IP address of a management station to be permitted SNMP access to the switch through the community string. You use this parameter when you give a community string a closed status. A community string with a closed status can only be used by those management stations whose IP addresses have been assigned to the string.

A community string can have up to eight manager IP addresses, but only one can be assigned when a community string is created. To add IP addresses of management stations to an existing community string, see “ADD SNMP COMMUNITY” on page 130.

Examples

The following command creates the new community string “serv12” with read access level and an access status of open:

```
create snmp community=serv12 access=read open=yes
```

The following command creates the new community string “wind11” with read and write access level. To limit the use of the string, its access status is specified as closed and it is assigned the IP address of the management station that will use the string:

```
create snmp community=wind11 access=write open=no
manager=149.35.24.22
```

(The OPEN=NO parameter can be omitted from the example because closed status is the default for a new community string.)

This command creates a community string called "serv12" with a closed status. The command assigns the string the IP address of a management that can use the string and also receive SNMP traps:

```
create snmp community=serv12 access=write open=no
traphost=149.35.24.22 manager=149.35.24.22
```

AlliedWare Plus Command

Syntax

```
snmp-server community community rw|ro
```

Mode

Configure mode

Description

This AlliedWare Plus command is used to create new SNMPv1 and v2c community strings. You can specify the names of the community strings and their access levels, which can be RW for read-write or RO for read-only. This command differs from the standard command as follows:

- Community names cannot contain spaces.
- This command can only create community strings that are closed, meaning they are only available to workstations whose IP addresses are assigned to them.
- You cannot use this command to add manager or trap IP addresses to new community strings. For that, refer to the AlliedWare Plus command in "ADD SNMP COMMUNITY" on page 130.

Example

This example creates the new community string "stea2a" with an access level of read-write:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server community stea2a rw
```

DELETE SNMP COMMUNITY

AlliedWare Plus
Command
Available

Syntax

```
delete snmp community=”community” traphost=ipaddress
manager=ipaddress
```

Parameters

community — Specifies the SNMP community string on the switch to be modified. The community string must already exist on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character, such as an exclamation point. Otherwise, the quotes are optional.

traphost — Specifies the IP address of a trap receiver to be removed from the community string.

manager — Specifies the IP address of a management station to be removed from the community string.

Description

This command removes the IP addresses of trap receivers and management workstations from community strings.

The TRAPHOST parameter removes the IP address of a trap receiver from an SNMP community string. Once an IP address is removed, the switch will not send SNMP traps to the trap receiver represented by the address.

The MANAGER parameter removes the IP address of a management station from the community string. A management station removed from a community string with a closed status can no longer use SNMP and the community string to manage the switch. If you remove the last management station IP address from a community string with a closed status, no SNMP management station can access the switch using that community string.

Examples

The following command deletes the IP address 149.212.11.22 of a management station from the community string “private.”

```
delete snmp community=private
manager=149.212.11.22
```

The following command deletes the IP address 149.212.44.45 of a trap receiver from the community string "public."

```
delete snmp community=public traphost=149.212.44.45
```

AlliedWare Plus Command

Syntax

```
no snmp-server host ipaddress trap community_string|
informs community_string
```

Mode

Configure mode

Description

The IPADDRESS parameter specifies the IP address of a network node to be removed as a trap receiver or a manager of a community string. To remove a node that is a trap receiver, use the TRAP parameter to specify the community string where the IP address is assigned. To remove the node as a manager of a string, use the INFORMS parameter to specify the community string.

You cannot specify both the TRAP parameter and the INFORMS parameter in the same command. To remove an IP address that is a trap receiver and a manager of the same community string, you must enter this command twice.

Examples

This example removes the IP address 115.124.187.4 as a trap receiver from the private community string:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 115.124.187.4 trap
private
```

This example removes the IP address 124.112.32.7 as a manager from the community string "lpa124wan":

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server host 124.112.32.7 informs
lpa124wan
```

This example removes the IP address 121.172.21.14 as both a trap receiver and a manager from the community string "wadt27:"

```
awplus> enable
awplus# configure terminal
```

```
awplus(config)# no snmp-server host 121.172.21.14 trap
wadt27
awplus(config)# no snmp-server host 121.172.21.14 informs
wadt27
```

DESTROY SNMP COMMUNITY

AlliedWare Plus Command Available

Syntax

```
destroy snmp community="community"
```

Parameter

community	Specifies an SNMP community string to delete from the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or special character, such as an exclamation point. Otherwise, the quotes are optional.

Description

This command deletes SNMP community strings from the switch. The IP addresses of management stations and SNMP trap receivers assigned to a deleted community string are deleted as well.

Example

This command deletes the community string “wind44”:

```
destroy snmp community=wind44
```

AlliedWare Plus Command

Syntax

```
no snmp-server community community
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example deletes the “pla178ta” community string:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server community pla178ta
```

DISABLE SNMP

AlliedWare Plus
Command
Available

Syntax

```
disable snmp
```

Parameters

None.

Description

This command disables SNMP on the switch. You cannot manage the unit from an SNMP management station when SNMP is disabled. The default setting for SNMP is disabled. This command does not affect the status of authentication failure traps. To disable the traps, refer to “DISABLE SNMP AUTHENTICATETRAP” on page 141.

Example

The following command disables SNMP on the switch:

```
disable snmp
```

AlliedWare Plus Command

Syntax

```
no snmp-server enable trap
```

Mode

Configure mode

Description

This AlliedWare Plus command disables both SNMP and authentication failure traps. The standard commands have a separate command for disabling authentication failure traps.

Example

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

DISABLE SNMP AUTHENTICATETRAP

Syntax

```
disable snmp authenticatetrap|authenticate_trap
```

Parameters

None.

Description

This command stops the switch from sending authentication failure traps to trap receivers. However, the switch will continue to send other system traps, such as alarm traps. The default setting for sending authentication failure traps is disabled.

The AUTHENTICATETRAP and AUTHENTICATE_TRAP keywords are equivalent.

To activate the authentication failure trap, refer to “ENABLE SNMP AUTHENTICATETRAP” on page 144.

Example

The following command instructs the switch not to send authentication failure traps to SNMP trap receivers:

```
disable snmp authenticatetrap
```

DISABLE SNMP COMMUNITY

Syntax

```
disable snmp community="community"
```

Parameter

community	Specifies an SNMP community string to disable on the switch. This parameter is case sensitive. The string must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.

Description

This command disables a community string on the switch, while leaving SNMP and all other community strings active. IP addresses of management stations or trap receivers assigned to the community string are also disabled. A disabled community string cannot be used by a management station to access the switch.

Example

The following command deactivates the SNMP community string “sw1200” and the IP addresses of any management stations and trap receivers assigned to the community string:

```
disable snmp community=sw1200
```

ENABLE SNMP

AlliedWare Plus
Command
Available

Syntax

```
enable snmp
```

Parameters

None.

Description

This command activates SNMP on the switch so that you can remotely manage the unit with an SNMP application program from a management station on your network. It also enables the switch to send SNMP traps to trap receivers. The default setting for SNMP on the switch is disabled.

This command does not affect the status of authentication failure traps. To enable the traps, refer to “ENABLE SNMP AUTHENTICATETRAP” on page 144.

Example

The following command activates SNMP on the switch:

```
enable snmp
```

AlliedWare Plus Command

Syntax

```
snmp-server enable trap
```

Mode

Configure mode

Description

This AlliedWare Plus command enables both SNMP and authentication failure traps. The standard commands have a separate command for enabling authentication failure traps.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server enable trap
```

ENABLE SNMP AUTHENTICATETRAP

Syntax

```
enable snmp authenticatetrap|authenticate_trap
```

Parameters

None.

Description

This command configures the switch to send authentication failure traps to trap receivers. The switch sends an authentication failure trap whenever a SNMP management station attempts to access the switch using an incorrect or invalid community string, or the management station’s IP address has not been added to a community string that has a closed access status.

The default setting for sending authentication failure traps is disabled. Refer to “ADD SNMP COMMUNITY” on page 130 to enter the IP addresses of the SNMP trap receivers.

The AUTHENTICATETRAP and AUTHENTICATE_TRAP keywords are equivalent.

Example

The following command configures the switch to send authentication failure traps to SNMP trap receivers:

```
enable snmp authenticatetrap
```

ENABLE SNMP COMMUNITY

Syntax

```
enable snmp community="community"
```

Parameter

community	Specifies an SNMP community string. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.

Description

This command activates a community string on the switch. The default setting for a new community string is enabled. You can use this command to enable a community string that you disabled with the DISABLE SNMP COMMUNITY command.

Example

The following command enables the SNMP community string “private”:

```
enable snmp community=private
```

SET SNMP COMMUNITY

Syntax

```
set snmp community="community" [access=read|write]
[open=yes|no|on|off|true|false]
```

Parameters

community — Specifies the SNMP community string whose access level or access status is to be changed. This community string must already exist on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional.

access — Specifies the new access level. Options are “read” for read only access and “write” for both read and write access. If no access level is specified, the default is “read.”

open — Specifies the open or closed access status of the community string. The options are:

- yes, on, true — The community string is open, meaning that any management station can use the string to access the switch. These options are equivalent.
- no, off, false — The community string is closed, meaning that only those management stations whose IP addresses are assigned to the string can use it to access the switch. To add IP addresses of management stations to a community string, refer to “ADD SNMP COMMUNITY” on page 130. The default setting for a community string is closed. These options are equivalent.

Description

This command changes the access level and access status of an existing SNMP community string.

Examples

The following command changes the access status for the SNMP community string “sw44” to closed:

```
set snmp community=sw44 open=no
```

The following command changes the access level for the SNMP community string “serv12” to read and write with open access:

```
set snmp community=serv12 access=write open=yes
```

SHOW SNMP

AlliedWare Plus Command Available

Syntax

```
show snmp [community="community"]
```

Parameter

community Specifies a community string on the switch. This parameter is case sensitive. The name must be enclosed in double quotes if it contains a space or other special character such as an exclamation point. Otherwise, the quotes are optional. Default community strings are “public” and “private.”

Description

This command displays the following SNMP information:

- SNMP status - The status will be enabled or disabled. If enabled, you can manage the switch with an SNMP application program from a remote management station. If disabled, you cannot remotely manage the switch using SNMP. The default for SNMP is disabled. To enable SNMP, refer “ENABLE SNMP” on page 143. To disable SNMP, refer to “DISABLE SNMP” on page 140.
- Authentication failure traps - This status will be enabled or disabled. If enabled, the switch sends out authentication failure traps to trap receivers. If disabled, the switch will not send out authentication failure traps, but will send out other system traps. The switch sends an authentication failure trap whenever a SNMP management station attempts to access the switch using an incorrect or invalid community string, or the management station’s IP address has not been added to a community string that has a closed access status. The default setting is enabled.

  To enable authentication failure traps, refer to “ENABLE SNMP AUTHENTICATETRAP” on page 144. To disable the sending of this trap, see “DISABLE SNMP AUTHENTICATETRAP” on page 141. To add IP addresses of management stations to receive the trap, refer to the “ADD SNMP COMMUNITY” on page 130.
- SNMP community strings - The switch comes with the two default community strings public, which has read access, and private, which has read and write access. To add new community strings, see “CREATE SNMP COMMUNITY” on page 133. To delete community strings, refer to “DESTROY SNMP COMMUNITY” on page 139.
- Management station IP addresses - These are the IP addresses of management stations that can access the switch through a community

string that has a closed access status. (Management station IP addresses are displayed only when you specify a specific community string using the COMMUNITY parameter in this command.) To add IP addresses of management stations to a community string, refer to "ADD SNMP COMMUNITY" on page 130.

- ❒ Trap receiver IP addresses - These are the IP addresses of management stations to receive SNMP traps from the switch. (IP addresses or trap receivers are displayed only when you specify a specific community string using the COMMUNITY parameter in this command.) To add IP addresses to a community string, refer to "ADD SNMP COMMUNITY" on page 130.
- ❒ Access Status - If a community string shows an Open Access with Yes, the string has an open access status, meaning any management stations can use the string. A string with a Open Access of No has a closed access status; only those management stations whose IP addresses have been assigned to the string can use it. To change the access status, refer to "SET SNMP COMMUNITY" on page 146.

Examples

The following command displays the SNMP status and the community strings on the switch:

```
show snmp
```

The following command displays specific information about the "private" community string. The information includes the IP addresses of management stations that can use the string and the IP addresses of SNMP trap receivers:

```
show snmp community=private
```

AlliedWare Plus Command

Syntax

```
show snmp-server community
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the same information as the standard command, but it does not have an option for specifying an individual community string.

Example

```
show snmp-server community
```

Chapter 8

Port Parameter Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ACTIVATE SWITCH PORT

Syntax

```
activate switch port=port autonegotiate
```

Parameter

port	Specifies a port. You can activate more than one port at a time.

Description

This command prompts a port that is using Auto-Negotiation to renegotiate its settings with its end node. The command can be helpful if you believe that a port and an end node have not successfully negotiated their settings.

Example

This command forces ports 1 and 4 to renegotiate their speed and duplex mode:

```
activate switch port=1,4 autonegotiate
```

DISABLE INTERFACE LINKTRAP

Syntax

```
disable interface=port linktrap
```

Parameter

port	Specifies the port on which you want to disable SNMP link traps. You can configure more than one port at a time.

Description

This command disables SNMP link traps on a port. When disabled, the switch does not send an SNMP link trap when there is a change to the status of a link on a port.

Note
In order for the switch to send SNMP traps to SNMP trap receivers, you must activate SNMP on the unit and specify one or more trap receivers.

Example

The following command disables link traps on port 21:

```
disable interface=21 linktrap
```

DISABLE SWITCH PORT

AlliedWare Plus Command Available

Syntax

```
disable switch port=port
```

Parameter

port	Specifies the port to disable. You can disable more than one port at a time.

Description

This command disables a port. When a port is disabled, it stops forwarding traffic. The default setting for a port is enabled.

Example

The following command disables ports 12 and 24:

```
disable switch port=12,24
```

Equivalent Command

```
set switch port=port status=disable
```

For information, see “SET SWITCH PORT” on page 162.

AlliedWare Plus Command

Syntax

```
shutdown
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example disables ports 15 and 16:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15,16
awplus(config-if)# shutdown
```

DISABLE SWITCH PORT FLOW

AlliedWare Plus
Command
Available

Syntax

```
disable switch port=port flow=pause
```

Parameter

port Specifies the port where you want to deactivate flow control. You can configure more than one port at a time.

Description

This command deactivates flow control on a port. Flow control only applies to ports operating in full duplex mode.

Example

The following command deactivates flow control on port 6:

```
disable switch port=6 flow=pause
```

Equivalent Command

```
set switch port=port flowcontrol=disable
```

For information, see “SET SWITCH PORT” on page 162.

AlliedWare Plus Command

Syntax

```
flowcontrol receive|send off
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example disables flow control on ports 18 to 21 and 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18-21,24
awplus(config-if)# flowcontrol receive off
```

This example deactivates flow control on port 19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 19
awplus(config-if)# flowcontrol receive off
```

ENABLE INTERFACE LINKTRAP

Syntax

```
enable interface=port linktrap
```

Parameter

port	Specifies the port on which you want to enable SNMP link traps. You can configure more than one port at a time.

Description

This command activates SNMP link traps on the port. When enabled, the switch sends an SNMP link trap to an SNMP trap receiver whenever there is a change to the status of a link on a port.

Note
Before the switch can send SNMP traps, you must activate SNMP on the unit and specify one or more trap receivers.

Example

The following command enables link traps on port 21:

```
enable interface=21 linktrap
```

ENABLE SWITCH PORT

AlliedWare Plus Command Available

Syntax

```
enable switch port=port
```

Parameter

port

Specifies the port to enable. You can configure more than one port at a time.

Description

This command enables a port. When a port is enabled, it forwards traffic. The default setting for a port is enabled.

Example

The following command enables ports 1 to 4:

```
enable switch port=1-4
```

Equivalent Command

```
set switch port=port status=enable
```

For information, see “SET SWITCH PORT” on page 162.

AlliedWare Plus Command

Syntax

```
no shutdown
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example enables port 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22
awplus(config-if)# no shutdown
```

ENABLE SWITCH PORT FLOW

AlliedWare Plus
Command
Available

Syntax

```
enable switch port=port flow=pause
```

Parameter

port	Specifies the port where you want to activate flow control. You can configure more than one port at a time.

Description

This command activates flow control on a port. Flow control only applies to ports operating in full duplex mode. When flow control is activated, a port sends out PAUSE packets when it wants the end node to stop sending packets.

Example

The following command activates flow control on port 5:

```
enable switch port=5 flow=pause
```

Equivalent Command

```
set switch port=port flowcontrol=enable
```

For information, see “SET SWITCH PORT” on page 162.

AlliedWare Plus Command

Syntax

```
flowcontrol receive|send on
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example activates flow control on ports 18 to 21 and 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18-21,24
awplus(config-if)# flowcontrol receive on
```

PURGE SWITCH PORT

Syntax

```
purge switch port=port
```

Parameters

port	Specifies the port whose parameter settings are to be returned to the default values. You can configure more than one port at a time.

Description

This command returns all of the parameter settings of a port to the factory default values. To reset a port and retain its settings, use "RESET SWITCH PORT" on page 161.

Example

The following example resets the settings for port 10 to the factory default values:

```
purge switch port=10
```

RESET SWITCH PORT

Syntax

```
reset switch port=port
```

Parameter

port	Specifies the port to reset. You can reset more than one port at a time.

Description

This command resets a port. The reset takes less that a second to complete. You might reset a port if it is experiencing a problem establishing a link with its end node. The port retains its current operating parameter settings. To reset a port to the factory default settings, use “PURGE SWITCH PORT” on page 160.

Example

The following command resets ports 5 to 8:

```
reset switch port=5-8
```

Equivalent Command

```
set switch port=port softreset
```

For information, see “SET SWITCH PORT” on page 162.

SET SWITCH PORT

AlliedWare Plus Command Available

Syntax

```
set switch port=port [description="description"]
[status=enabled|disabled]
[speed=autonegotiate|10mhalf|10mfull|100mhalf|100mfull|
1000mfull]
[mdimode=mdi|mdix|auto]
[flowcontrol=disable|enable|auto]
[fctrllimit=value]
[backpressure=yes|no|on|off|true|false|enabled|
disabled]
[bplimit=value]
[holbplimit=value]
[renegotiation=auto]
[softreset]
```

Parameters

port
: Specifies the port to be configured. You can configure more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command.

description
: A description for the port, from 1 to 15 alphanumeric characters. Spaces are allowed, but not special characters. A description that contains spaces must be enclosed in double quotes. Otherwise, the quotes are optional. You cannot specify a description when configuring more that one port.

status
: Specifies the operating status of the port. The options are:

enabled — The port forwards network traffic. This is the default setting.

disabled — The port does not forward network traffic.

speed
: Sets the speed and duplex mode of the port. The options are:

autonegotiate — The port uses Auto-Negotiation for both speed and duplex mode. This is the default setting.

10mhalf — 10 Mbps and half-duplex mode.

10mfull 10 Mbps and full-duplex mode.

100mhalf 100 Mbps and half-duplex mode.

100mfull 100 Mbps and full-duplex mode.

1000mfull 1000 Mbps and full-duplex mode. (Applies only to 1000Base SFP and GBIC modules. This selection should not be used. An SFP or GBIC module should use Auto-Negotiation to set its speed and duplex mode.)

Note
A 10/100/1000Base-T twisted pair port must be set to Auto-Negotiation to operate at 1000 Mbps.

mdimode Sets the wiring configuration of the port. This parameter applies to twisted pair ports, and only when a port’s speed and duplex mode are set manually. If a port is autonegotiating its speed and duplex mode, the MDI/MDIX setting is established automatically and cannot be changed. The options are:

mdi Sets the port’s configuration to MDI.

mdix Sets the port’s configuration to MDI-X.

flowcontrol Specifies the flow control on the port. Flow control applies only to ports operating in full duplex mode. When flow control is activated, a port sends out a PAUSE packet whenever it wants the end node to stop sending packets. The options are:

disabled No flow control. This is the default setting.

enabled Flow control is activated.

fctrllimit Specifies the number of cells for flow control. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

backpressure Controls backpressure on the port. Backpressure applies only to ports operating in half-duplex mode. The options are:

yes, on, true, enabled — Activates backpressure on the port. These options are equivalent.

no, off, false, disabled — Deactivates backpressure on the port. This is the default. These options are equivalent.

bplimit — Specifies the number of cells for backpressure. A cell represents 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.

holbplimit — Specifies the threshold at which the switch signals a head of line blocking event on a port. The threshold is specified in cells. A cell is 128 bytes. The range is 1 to 61,440 cells; the default is 7,168.

renegotiation — Prompts the port to renegotiate its speed and duplex mode with the end node. This parameter only works when the port is using Auto-Negotiation. The only option is:

auto — Renegotiates speed and duplex mode with the end node.

softreset — Resets the port. This parameter does not change any of a port’s operating parameters.

Description

This command configures the operating parameters of a port. You can set more than one parameter at a time.

Examples

The following command disables ports 1 to 6:

```
set switch port=1-6 status=disabled
```

The following command configures port 8 to operate at 10 Mbps, half duplex:

```
set switch port=8 speed=10mhalf
```

The following command sets the speed on ports 2 to 6 to 100 Mbps, the duplex mode to full duplex, the wiring configuration to MDI-X, and flow control to enabled:

```
set switch port=2-6 speed=100mfull mdimode=mdix
flowcontrol=enabled
```

The following command resets port 5:

```
set switch port=5 softreset
```

Equivalent Commands

```
disable switch port=port
```

For information, see “DISABLE SWITCH PORT” on page 154.

```
disable switch port=port flow=pause
```

For information, see “DISABLE SWITCH PORT FLOW” on page 155.

```
enable switch port=port
```

For information, see “ENABLE SWITCH PORT” on page 158.

```
enable switch port=port flow=pause
```

For information, see “ENABLE SWITCH PORT FLOW” on page 159.

```
reset switch port=port
```

For information, see “RESET SWITCH PORT” on page 161.

AlliedWare Plus Command

Syntax

To set a port’s speed:

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

To set a port’s MDI/MDIX setting:

```
polarity mdi|mdix
```

To set a port’s description:

```
description description
```

This command does not accept spaces in the description.

To return a port’s description to the default value:

```
no description
```

To disable a port:

```
shutdown
```

To enable a port:

```
no shutdown
```

To enable or disable flow control:

```
flowcontrol receive|send on|off
```

To enable or disable backpressure:

```
flowcontrol backpressure on|off
```

To specify the threshold for flow control and backpressure:

```
bplimit value
```

or

```
fctrllimit value
```

To specify the threshold for head of line blocking events:

```
holbplimit value
```

To prompt a port set to Auto-Negotiation to renegotiate its speed and duplex mode with an end node.

```
renegotiate
```

To perform a software reset:

```
softreset
```

Mode

Port Interface mode

Description

These AlliedWare Plus commands perform all the same functions as the standard command.

Examples

This example sets the speeds on ports 11 and 17 to 100Mbps, half-duplex:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11,17
awplus(config-if)# speed 100mhalf
```

This example activates Auto-Negotiation on port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15
awplus(config-if)# speed auto
```

This example sets the wiring configuration for port 28 to MDI:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 28
awplus(config-if)# polarity mdi
```

This example activates backpressure on port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15
awplus(config-if)# flowcontrol backpressure on
```

This example activates flow control on ports 11 and 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11,18
awplus(config-if)# flowcontrol receive on
awplus(config-if)# flowcontrol send on
```

This example sets the threshold for flow control and backpressure on ports 15 and 20 to 7000 cells:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15,20
awplus(config-if)# bplimit 7000
```

This example performs a soft reset on ports 18 to 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18-21
awplus(config-if)# softreset
```

To set the wiring configuration on a port, you must disable Auto-Negotiation and set the speed and duplex mode manually.

This example assigns the name “printer22” to port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15
awplus(config-if)# description printer22
```

The description of a port cannot contain spaces.

This example disables port 3:

```
awplus> enable
```

```
awplus# configure terminal
awplus(config)# interface 3
awplus(config-if)# shutdown
```

This example enables port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5
awplus(config-if)# no shutdown
```

This example sets the head of line blocking threshold on port 9 to 5,000 cells:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 9
awplus(config-if)# holbplimit 5000
```

This example activates flow control on ports 18 to 21 and 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18-21,24
awplus(config-if)# flowcontrol receive on
```

This example deactivates flow control on port 19:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 19
awplus(config-if)# flowcontrol receive off
```

This example activates backpressure on ports 4 and 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 4,8
awplus(config-if)# flowcontrol backpressure on
```

This example deactivates backpressure on ports 1 to 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 1-4
awplus(config-if)# flowcontrol backpressure off
```

This example performs a software reset on ports 7 and 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 7,8
awplus(config-if)# softreset
```

SET SWITCH PORT FILTERING

AlliedWare Plus Command Available

Syntax

```
set switch port=port
[bcastfiltering=yes|no|on|off|true|false|enabled|
disabled]
[bcastegressfiltering=yes|no|on|off|true|false|enabled|
disabled]
[unkmcastfiltering=yes|no|on|off|true|false]
[unkmcastegressfiltering=yes|no|on|off|true|false]
[unkucastfiltering=yes|no|on|off|true|false]
[unkucastegressfiltering=yes|no|on|off|true|false]
```

Parameters

port — Specifies the port you want to configure. You can configure more than one port at a time.

bcastfiltering — Controls the ingress broadcast frame filter. The options are:

yes, on, true, enabled — The port discards all ingress broadcast frames. These options are equivalent.

no, off, false, disabled — The port forwards all ingress broadcast frames. This is the default. These options are equivalent.

bcastegressfiltering — Controls the egress broadcast frame filter. The options are:

yes, on, true, enabled — The port discards all egress broadcast frames. These options are equivalent.

no, off, false, disabled — The port forwards all egress broadcast frames. This is the default. These options are equivalent.

unkmcastfiltering — Controls the unknown ingress multicast frame filter. The options are:

yes, on, true, enabled — The port discards all

		unknown ingress multicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown ingress multicast frames. This is the default. These options are equivalent.
unkmcastegressfiltering	Controls the unknown egress multicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown egress multicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown egress multicast frames. These options are equivalent.
unkucastfiltering	Controls the unknown ingress unicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown ingress unicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown ingress unicast frames. This is the default. These options are equivalent.
unkucastegressfiltering	Controls the unknown egress unicast frame filter. The options are:	
	yes, on, true, enabled	The port discards all unknown egress unicast frames. These options are equivalent.
	no, off, false, disabled	The port forwards all unknown egress unicast frames. This is the default. These options are equivalent.

Description

This command discards ingress and egress broadcast packets as well as unknown unicast and multicast packets on a port. When you activate this feature on a port, the port discards all ingress or egress packets of the type specified. The default setting for each type of packet filter is disabled.

Examples

The following command activates the ingress broadcast filter on ports 4 and 23 so that the ports discard all ingress broadcast packets:

```
set switch port=4,23 bcastfiltering=yes
```

The following command activates the unknown egress multicast and unicast filters on ports 3 and 6 so that the ports discard all unknown egress multicast and unicast packets:

```
set switch port=3,6 unkmcastegressfiltering=yes
unkucastegressfiltering=yes
```

This command disables the unknown ingress unicast filter on port 24 so that the port again accepts all unknown ingress unicast packets:

```
set switch port=24 unkucastfiltering=no
```

AlliedWare Plus Command

Syntax

To activate the ingress broadcast frame filter:

```
filtering broadcast ingress
```

To activate the egress broadcast frame filter:

```
filtering broadcast egress
```

To activate the unknown ingress multicast frame filter:

```
filtering multicast ingress
```

To activate the unknown egress multicast frame filter:

```
filtering multicast egress
```

To activate the unknown ingress unicast frame filter:

```
filtering dlf ingress
```

To activate the unknown egress unicast frame filter:

```
filtering dlf egress
```

To disable a filter, use the NO form of the command.

Mode

Port Interface mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example activates the ingress broadcast filter on ports 18 and 21. The ports discard all ingress broadcast packets:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18,21
awplus(config-if)# filtering broadcast ingress
```

This example activates the unknown egress multicast filter on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 4
awplus(config-if)# filtering multicast egress
```

This example activates the unknown ingress unicast filter on ports 2 to 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2-7
awplus(config-if)# filtering dlf ingress
```

This example disables the ingress broadcast filter on port 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 8
awplus(config-if)# no filtering broadcast ingress
```

This example disables the unknown egress multicast filter on ports 15 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15,17
awplus(config-if)# no filtering multicast egress
```

SET SWITCH PORT RATELIMITING

AlliedWare Plus
Command
Available

Syntax

```
set switch port=port
[bcastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[bcastrate=value]
[mcastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[mcastrate=value]
[unkucastratelimiting=yes|no|on|off|true|false|enabled|
disabled]
[unkucastrate=value]
```

Parameters

port
Specifies the port you want to configure. You can configure more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command.

bcastratelimiting
Enables or disables rate limit for ingress broadcast packets. The options are:

yes, on, true, enabled
Activates broadcast packet rate limiting on the port. The options are equivalent. The rate limit is set with the BCASTRATE parameter.

no, off, false, disabled
Deactivates broadcast packet rate limit on the port. This is the default. The options are equivalent.

bcastrate
Specifies the maximum number of ingress broadcast packets a switch port accepts each second. The range is 0 to 262,143 packets. The default is 262,143 packets

mcastratelimiting
Enables or disables a rate limit for ingress multicast packets. The options are:

yes, on, true, enabled
Activates multicast packet rate limit on the port. The options are equivalent.

no, off, false, disabled — Deactivates multicast packet rate limit on the port. This is the default. The options are equivalent.

mcastrate — Specifies the maximum number of ingress multicast packets a switch port accepts each second. The range is 0 to 262,143 packets. The default is 262,143 packets.

unkucastratelimiting — Enables or disables rate limit for unknown ingress unicast packets. The options are:

yes, on, true, enabled — Activates unknown unicast packet rate limit on the port. The options are equivalent.

no, off, false, disabled — Deactivates unknown unicast packet rate limit on the port. This is the default. The options are equivalent.

unkucastrate — Specifies the maximum number of ingress unknown unicast packets a switch port accepts each second. The range is 0 to 262,143 packets. The default is 262,143 packets.

Description

This command sets the maximum number of ingress packets a port accepts each second. Packets exceeding the threshold are discarded. You can enable the rate limiting threshold independently for broadcast, multicast and unknown unicast packets.

Examples

The following command activates rate limiting for ingress broadcast and multicast packets on port 6. It sets a threshold of 20,000 packets per second for broadcast packets and 100,000 for multicast packets:

```
set switch port=6 bcastratelimiting=yes bcastrate=20000
mcastratelimiting=yes mcastrate=100000
```

The following command sets a threshold of 150,000 packets per second for unknown ingress unicast packets on ports 15 and 17:

```
set switch port=15,17 unkucastratelimiting=yes
unkucastrate=150000
```

The following command disables the rate limiting feature for ingress broadcast packets on port 24:

```
set switch port=24 bcastratelimiting=no
```

AlliedWare Plus Command

Syntax

To activate rate limiting for broadcast packets:

```
storm-control broadcast level value
```

To activate rate limiting for multicast packets:

```
storm-control multicast level value
```

To activate rate limiting for unknown unicast packets:

```
storm-control dlf level value
```

To disable rate limiting and to return the rate values to their default settings:

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

Mode

Port Interface mode

Description

These commands are equivalent to the standard command.

Examples

This example sets a threshold of 5,000 packets per second for ingress broadcast packets on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 12
awplus(config-if)# storm-control broadcast level 5000
```

This example sets a threshold of 100,000 packets per second for ingress multicast packets on port 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 4
awplus(config-if)# storm-control multicast level 100000
```

This example sets a threshold of 200,000 packets per second for ingress unknown unicast packets on ports 15 and 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15,17
awplus(config-if)# storm-control dlf level 200000
```

This example disables broadcast rate limiting on port 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 12
awplus(config-if)# no storm-control broadcast
```

This example disables multicast rate limiting on port 23:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 23
awplus(config-if)# no storm-control multicast
```

This example disables unknown unicast rate limiting on port 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5
awplus(config-if)# no storm-control dlf
```

SHOW INTERFACE

Syntax

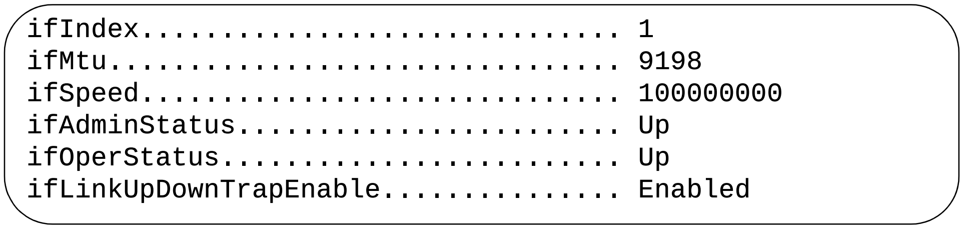
```
show interface[=port]
```

Parameter

port Specifies the port whose interface information you want to display. You can display more than one port at a time. To display all of the ports, do not include a port number.

Description

This command displays the contents of the interface MIB for a specific port. An example of the information displayed by this command is shown in Figure 35.



```
ifIndex............................. 1
ifMtu............................... 9198
ifSpeed............................. 100000000
ifAdminStatus....................... Up
ifOperStatus........................ Up
ifLinkUpDownTrapEnable.............. Enabled
```

Figure 35. SHOW INTERFACE Command

This command provides the following information about a port:

- ifIndex - The index of the interface in the interface table.
- ifMTU - The size, in octets, of the largest packet that can be transmitted on the port.
- ifSpeed - An estimate of the port's current bandwidth, in bits per second. This MIB object is zero (0) when the port does not have a link to an end node.
- ifAdminStatus - The configured state of the port, one of the following:

  Up - The port is up.

  Down - The port is down.

- ifOperStatus - The current operational status of the port, one of the following:

  Up - A valid link exists between the port and the end node.

  Down - The port and the end node have not established a link.

unknown - The port status is unknown.

- ifLinkUpDownTrapEnable - Whether or not link traps have been enabled for the port, one of the following:

  Enabled - Link traps are enabled. To disable link traps, see “DISABLE INTERFACE LINKTRAP” on page 153.

  Disabled - Link traps are disabled. To enable link traps, see “ENABLE INTERFACE LINKTRAP” on page 157.

Example

The following command displays information about port 21:

```
show interface=21
```

SHOW SWITCH PORT

AlliedWare Plus Command Available

Syntax

```
show switch port[=port]
```

Parameter

port — Specifies the port whose parameter settings you want to view. You can display more than one port at a time. To display all of the ports, do not include a port number.

Description

This command displays a port’s current operating specifications, such as speed and duplex mode. The command displays the following port information. (For an example of the information displayed by this command, see Figure 36 on page 183.)

- Port Description - Displays the name of the port. The default name is “Port_” followed by the port number. To configure a port’s name, refer to “SET SWITCH PORT” on page 162.
- Port Type - Displays the IEEE standard of a port. For example, the port type for a twisted pair port on an AT-9424T/SP switch is 10/100/1000Base-T.
- Status - Displays whether the port is currently enabled or disabled. When disabled, a port does not forward network traffic. The default is enabled. To disable or enable a port, refer to “DISABLE SWITCH PORT” on page 154, “ENABLE SWITCH PORT” on page 158, or “SET SWITCH PORT” on page 162.
- Link State - Displays the current link state between the port and the end node. If the port has established a link with an end node, link state will be “Up.” If there is no link, link state will be “Down.”
- Configured Speed/Duplex - Displays the current configured settings for speed and duplex mode on the port. The setting of “Auto” indicates the port has been set to Auto-Negotiation, the default setting. To adjust a port’s speed and duplex mode, refer to “SET SWITCH PORT” on page 162.
- Configured MDI Crossover - Displays the current configured setting for MDI/MDIX on the port. If the port is set to Auto-Negotiation, this field displays N/A, because the MDI/MDIX setting is set automatically on the port. A value only appears in this field if you disable Auto-Negotiation on a twisted pair port and set MDI/MDIX manually. This field does not apply to a fiber optic port. To adjust a port’s MDI/MDIX setting, refer to “SET SWITCH PORT” on page 162.

- ❒ Actual Speed/Duplex - Displays the current operating speed and duplex mode of a port. This field displays no value (—) if the port does not have a link to an end node or has been disabled.
- ❒ Actual MDI Crossover- Displays the current operating MDI/MDIX setting of a twisted pair port. This field displays no value (—) if the port does not have a link to an end node or has been disabled. This field does not apply to a fiber optic port.
- ❒ Flow Control Status and Flow Control Threshold - Displays the status of flow control on a port. Flow control applies to ports operating in full duplex mode and is used by a port to stop an end node from sending packets when its ingress buffer is full. The default setting is disabled. The threshold marks the point at which flow control is activated. The threshold is measured in cells of 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.To set flow control, refer to "DISABLE SWITCH PORT FLOW" on page 155, "ENABLE SWITCH PORT FLOW" on page 159, or "SET SWITCH PORT" on page 162.
- ❒ Backpressure Status and Backpressure Threshold - Displays the status of backpressure on a port. Backpressure applies to ports operating in half duplex mode. A port uses backpressure to stop an end node from sending packets when its ingress buffer is full. The default setting is disabled. The threshold marks the point at which backpressure is activated. The threshold is measured in cells of 128 bytes. The range is 1 to 7935 cells. The default value is 7935 cells.To set backpressure, refer to "SET SWITCH PORT" on page 162.
- ❒ HOL Blocking Prevention Threshold - Displays the threshold at which the switch signals a head of line blocking event. This event occurs when switch ports are unable to forward packets to another switch port because its egress queues are full. The switch responds to this event by instructing the other switch ports to discard any packets in their ingress queues that are destined for the oversubscribed port. The threshold is measured in cells of 128 bytes. The range is 0 to 8191 cells. The default is 682.
- ❒ Broadcast Ingress Filtering - Displays the status of ingress broadcast filtering. If enabled, the port discards all ingress broadcast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 169.
- ❒ Broadcast Egress Filtering - Displays the status of egress broadcast filtering. If enabled, the port discards all egress broadcast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 169.
- ❒ Unknown Multicast Ingress Filtering - Displays the status of unknown ingress multicast filtering. If enabled, the port discards all unknown ingress multicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 169.
- ❒ Unknown Multicast Egress Filtering - Displays the status of unknown egress multicast filtering. If enabled, the port discards all unknown

egress multicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 169.

- ❐ Unknown Unicast Ingress Filtering - Displays the status of unknown ingress unicast filtering. If enabled, the port discards all unknown ingress unicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 169.
- ❐ Unknown Unicast Egress Filtering - Displays the status of unknown egress unicast filtering. If enabled, the port discards all unknown egress unicast packets. The default is disabled. To configure this parameter, refer to "SET SWITCH PORT FILTERING" on page 169.
- ❐ Broadcast Rate Limiting Status and Broadcast Rate - Displays the status of the broadcast rate limiting feature. If enabled, the port limits the number of ingress broadcast packets per second to the rate specified. Ingress broadcast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to "SET SWITCH PORT RATELIMITING" on page 173.
- ❐ Multicast Rate Limiting Status and Multicast Rate - Displays the status of the multicast rate limiting feature. If enabled, the port limits the number of ingress multicast packets per second to the rate specified. Ingress multicast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to "SET SWITCH PORT RATELIMITING" on page 173.
- ❐ Unknown Unicast Rate Limiting Status and Unknown Unicast Rate - Displays the status of the unicast rate limiting feature. If enabled, the port limits the number of unknown ingress unicast packets per second to the rate specified. Unknown ingress unicast packets that exceed the threshold are discarded by the port. The default setting for this feature is disabled. The default rate is 262,143 packets per second. To set this feature, refer to "SET SWITCH PORT RATELIMITING" on page 173.
- ❐ PVID - Displays the port's VLAN ID number. This number is equivalent to the VID of the VLAN where the port is currently an untagged member. The default is 1, the VID of the Default_VLAN. To add a port to an existing VLAN or to create a new VLAN, refer to "ADD VLAN" on page 644 and "CREATE VLAN" on page 647.
- ❐ Port Priority - Displays the Class of Service priority assigned to the port. This priority level applies to all ingress untagged packets received on the port. The default setting is 0. At the default setting, all ingress untagged packets received on the port are stored in the egress port's Q1 egress queue. To set this parameter, refer to "SET SWITCH PORT PRIORITY OVERRIDEPRIORITY" on page 368. To adjust the mappings of priority levels to egress queues, see "SET QOS COSP" on page 365.
- ❐ Override Priority - Displays whether the Class of Service priority level in ingress tagged packets is ignored when determining the egress

queue for storing the packets. If this parameter is displaying Yes, the switch ignores the priority level in tagged packets and uses the priority level assigned to the port to determine the egress queue. The default setting is No. At the default setting the priority level in tagged packets is used to determine the appropriate egress queue. To set this parameter, refer to “SET SWITCH PORT PRIORITY OVERRIDEPRIORITY” on page 368. To adjust the mappings of priority levels to egress queues, see “SET QOS COSP” on page 365.

❒ Mirroring State - Displays the state of port mirroring on the switch. If port mirroring has been activated on the switch, this field will contain Enabled. If port mirroring has not been activated on the switch, the default setting, this field will contain Disabled. To configure port mirroring, refer to “SET SWITCH MIRROR” on page 238 and “SET SWITCH PORT MIRROR” on page 239.

❒ Is this mirror port mirror - Displays whether the port is functioning as the destination port of a port mirror. This field only appears if port mirroring has been activated on the switch. This field displays No if the port is not the destination port and Yes if it is the destination port.

Note
The information for an SFP or GBIC module includes additional nonadjustable operating specifications of the module.

An example of the information displayed by this command is shown in Figure 36 on page 183.

```
Port #11 Information:

Port Description ..................... Port_11
Port Type ............................ 10/100/1000Base-T
Status ............................... Enabled
Link State ........................... Up
Configured Speed/Duplex .............. Auto
Configured MDI Crossover ............. N/A
Actual Speed/Duplex .................. 100 Mbps/Full Duplex
Actual MDI Crossover ................. MDIX
Flow Control Status .................. Disabled
Flow Control Threshold ............... 7935 cells
Backpressure Status .................. Disabled
Backpressure Threshold ............... 7935 cells
HOL Blocking Prevention Threshold .... 682 cells
Broadcast Ingress Filtering .......... Disabled
Broadcast Egress Filtering ........... Disabled
Unknown Multicast Ingress Filtering .. Disabled
Unknown Multicast Egress Filtering ... Disabled
Unknown Unicast Ingress Filtering .... Disabled
Unknown Unicast Egress Filtering ..... Disabled
Broadcast Rate Limiting Status ....... Disabled
Broadcast Rate ....................... 262143 packet/second
Multicast Rate Limiting Status ....... Disabled
Multicast Rate ....................... 262143 packet/second
Unknown Unicast Rate Limiting Status . Disabled
Unknown Unicast Rate ................. 262143 packet/second
PVID ................................. 1
Port Priority (0-7) 0=Low 7=High...... 0
Override Priority .................... No
Mirroring State....................... Disabled
```

Figure 36. SHOW SWITCH PORT Command

Examples

The following command displays the settings for all the ports:

```
show switch port
```

The following command displays the settings for port 14:

```
show switch port=14
```

AlliedWare Plus Command

Syntax

```
show interface port
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

The following command displays the settings for ports 1 to 4:

```
awplus# show interface 1-4
```

Chapter 9

Port Statistics Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

RESET SWITCH PORT COUNTER

Syntax

```
reset switch port=port counter
```

Parameter

port	Specifies the port whose statistics counters you want to return to zero. You can specify more than one port in the command.

Description

This command returns a port’s statistics counters to zero.

Example

The following command returns the counters on ports 14 and 15 to zero:

```
reset switch port=14-15 counter
```

SHOW SWITCH MODULE COUNTER

Syntax

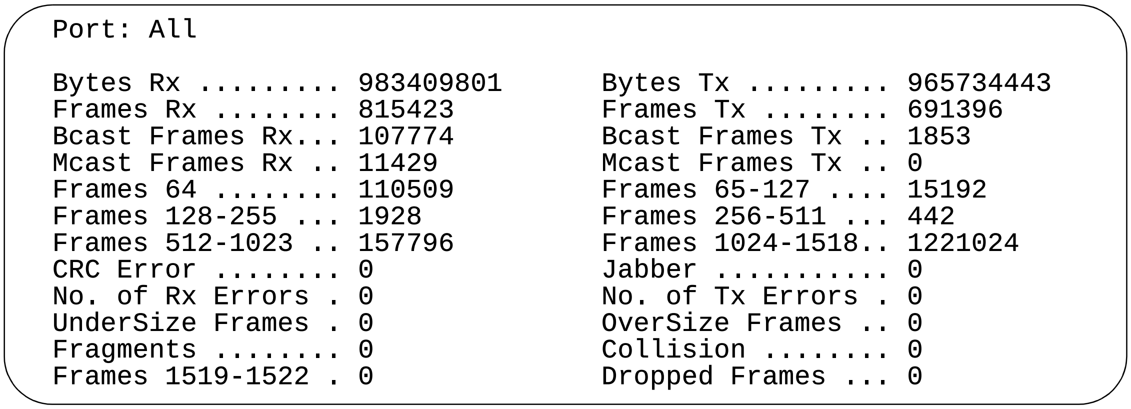
```
show switch module=id_number counter
```

Parameters

module Specifies the stack ID number of a switch. For a stand-alone switch, this number is 1. You can specify only one ID number at a time. To determine the stack ID number of a switch, refer to “SHOW STACK” on page 106.

Description

This command is used to display the operating statistics for stand-alone switches and for master and member switches in an AT-9400Ts Stack. The information includes the number of packets received and transmitted, and the number of CRC errors. An example of the display is shown in Figure 37.



```
Port: All

Bytes Rx ......... 983409801      Bytes Tx ......... 965734443
Frames Rx ........ 815423         Frames Tx ........ 691396
Bcast Frames Rx... 107774         Bcast Frames Tx .. 1853
Mcast Frames Rx .. 11429          Mcast Frames Tx .. 0
Frames 64 ........ 110509         Frames 65-127 .... 15192
Frames 128-255 ... 1928           Frames 256-511 ... 442
Frames 512-1023 .. 157796         Frames 1024-1518.. 1221024
CRC Error ........ 0              Jabber ........... 0
No. of Rx Errors . 0              No. of Tx Errors . 0
UnderSize Frames . 0              OverSize Frames .. 0
Fragments ........ 0              Collision ........ 0
Frames 1519-1522 . 0              Dropped Frames ... 0
```

Figure 37. SHOW SWITCH MODULE COUNTER Command

The command provides the following information:

Bytes Rx
Number of bytes received by the switch.

Bytes Tx
Number of bytes transmitted by the switch.

Frames Rx
Number of frames received by the switch.

Frames Tx
Number of frames transmitted by the switch.

Bcast Frames Rx
Number of broadcast frames received by the switch.

Bcast Frames Tx
Number of broadcast frames transmitted by the switch.

Mcast Frames Rx
Number of multicast frames received by the switch.

Mcast Frames Tx
Number of multicast frames transmitted by the switch.

Frames 64
Frames 65-127
Frames 128-255
Frames 256-511
Frames 512-1023
Frames 1024-1518
Frames 1519-1522
Number of frames transmitted from the switch, grouped by size.

CRC Error
Number of frames with a cyclic redundancy check (CRC) error but with the proper length (64-1518 bytes) received by the switch.

Jabber
Number of occurrences of corrupted data or useless signals appearing on the switch.

No. of Rx Errors
Number of receive errors.

No. of Tx Errors
Number of transmit errors.

Undersize Frames
Number of frames that were less than the minimum length specified by IEEE 802.3 (64 bytes including the CRC) received by the switch.

Oversize Frames
Number of frames exceeding the maximum specified by IEEE 802.3 (1518 bytes including the CRC) received by the switch.

Fragments
Number of undersized frames, frames with alignment errors, and frames with frame check sequence (FCS) errors (CRC errors) received by the switch.

Collision
Number of collisions that have occurred on the switch.

Dropped Frames
Number of frames successfully received and buffered by the switch, but discarded and not forwarded.

Examples

This command displays the operating statistics for a stand-alone switch or for a master switch of a stack:

```
show switch module=1 counter
```

This command displays the operating statistics for a member switch assigned the ID number 4 in a stack:

```
show switch module=4 counter
```

SHOW SWITCH PORT COUNTER

AlliedWare Plus
Command
Available

Syntax

```
show switch port=port counter
```

Parameter

port Specifies the port whose statistics you want to view. You can specify more than one port at a time. To view all ports, do not specify a port.

Description

This command displays the operating statistics for a port on the switch. Examples of the statistics include the number of packets transmitted and received, and the number of CRC errors. For an example of the display and definitions of the statistics, refer to “SHOW SWITCH MODULE COUNTER” on page 187.

Examples

The following command displays the operating statistics for port 14:

```
show switch port=14 counter
```

The following command displays the operating statistics for all the ports:

```
show switch port counter
```

AlliedWare Plus Command

Syntax

```
show statistics port
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

The following command displays the statistics for ports 21 and 23:

```
awplus# show statistics 21,23
```

Chapter 10

MAC Address Table Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD SWITCH FDB|FILTER

AlliedWare Plus
Command
Available

Syntax

```
add switch fdb|filter destaddress|macaddress=macaddress
port=port vlan=vlan-name|vid
```

Note
The FDB and FILTER keywords are equivalent.

Parameters

destaddress ***or*** macaddress
Specifies the static unicast or multicast address to be added to the switch’s MAC address table. The parameters are equivalent. The address can be entered in either of the following formats:

xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

port
Specifies the port(s) where the MAC address is to be assigned. You can specify only one port when adding a unicast address. You can specify more than one port when adding a multicast address.

vlan
Specifies the name or VID of the VLAN where the node designated by the MAC address is a member.

Description

This command is used to add static unicast and multicast MAC addresses to the switch’s MAC address table. A MAC address added with this command is never timed out from the MAC address table, even when the end node or, in the case of a multicast address, the multicast application is inactive.

If you are entering a static multicast address, you must assign the address to the port where the multicast application is located and to the ports where the host nodes are connected. The multicast packets will not be forwarded to the host nodes if you assign the address to only the port where the multicast application is located.

Examples

The following command adds the static MAC address 00:A0:D2:18:1A:11 to port 7. It assumes the port where the MAC address is to be assigned is a member of the Default_VLAN:

```
add switch fdb macaddress=00:A0:D2:18:1A:11 port=7
vlan=default_vlan
```

The following command adds the multicast MAC address 01:00:51:00:00 10 to ports 1 to 5 in the Engineering VLAN:

```
add switch fdb macaddress=01:00:51:00:00:10 port=1-5
vlan=Engineering
```

AlliedWare Plus Command

Syntax

mac address-table static *macaddress port vlan-name*|*vid*

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This command adds the static MAC address 4B:C3:22:17:62:A4 to port 4 in the Production VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table static 4b:c3:22:17:62:a4 4
Production
```

DELETE SWITCH FDB|FILTER

AlliedWare Plus
Command
Available

Syntax 1

```
delete switch fdb|filter
macaddress|destaddress=macaddress vlan=name|vid
```

Syntax 2

```
delete switch fdb|filter
type|status=static|staticunicast|staticmulticast|dynamic|
dynamicunicast|dynamicmulticast
```

> **Note**
> The FDB and FILTER keywords are equivalent.

Parameters

macaddress ***or*** destaddress

Deletes a dynamic or static unicast or multicast MAC address from the MAC address table. The address can be entered in either of the following formats:

xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

This parameter must be accompanied with the VLAN parameter.

vlan

Specifies the VLAN containing the port(s) where the address was learned or assigned. The VLAN can be specified by name or VID. This parameter must be used with the MACADDRESS and DESTADDRESS parameters.

type ***or*** status

Deletes specific types of MAC addresses. Options are:

static — Deletes all static unicast and multicast MAC addresses.

staticunicast — Deletes all static unicast addresses.

staticmulticast — Deletes all static multicast addresses.

dynamic — Deletes all dynamic unicast and multicast MAC addresses.

dynamicunicast — Deletes all dynamic unicast addresses.

dynamicmulticast	Deletes all dynamic multicast addresses.

Description

This command is used to delete dynamic and static unicast and multicast addresses from the switch's MAC address table.

The command has two syntaxes. The first syntax is used to delete specific MAC addresses from the table and the second syntax is used to delete general types of addresses.

> **Note**
> You cannot delete a switch's MAC address, an STP BPDU MAC address, or a broadcast address.

Examples

The following command deletes the static MAC address 00:A0:D2:18:1A:11 from the table. The port where the address was learned or assigned is part of the Default_VLAN, which has a VID of 1:

```
delete switch fdb macaddress=00:A0:D2:18:1A:11 vlan=1
```

The following command deletes the MAC address 00:A0:C1:11:22:44 from the table. The port where the address was learned or assigned is part of the Sales VLAN:

```
delete switch fdb macaddress=00:a0:c1:11:22:44 vlan=sales
```

The following command deletes all the dynamic MAC addresses:

```
delete switch fdb type=dynamic
```

The following command deletes all the static unicast MAC addresses:

```
delete switch fdb type=staticunicast
```

AlliedWare Plus Command

Syntax

no mac address-table static *macaddress vlan-name*|*vid*

Mode

Configure mode

Description

This command lets you delete static and dynamic MAC addresses from the MAC address table. You can delete only one address at a time. This command, unlike the standard command, does not have options to delete specific types of MAC addresses.

Example

This command deletes the MAC address 86:24:3c:79:52:32 in the Sales VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# no mac address-table static
86:24:3c:79:52:32 Sales
```

RESET SWITCH FDB

Syntax

```
reset switch fdb [port=port]
```

Parameter

port	Specifies the port whose dynamic MAC addresses are to be deleted from the MAC address table. You can specify more than one port at a time.

Description

You use this command to delete all the dynamic MAC addresses in the MAC address table or the addresses learned on a specific port. After a port’s dynamic MAC addresses have been deleted, the port begins to learn new addresses.

Examples

The following command deletes all the dynamic MAC addresses in the switch’s MAC address table:

```
reset switch fdb
```

The following command deletes all the dynamic MAC addresses learned on port 5:

```
reset switch fdb port=5
```

SET SWITCH AGINGTIMER|AGEINGTIMER

AlliedWare Plus Command Available

Syntax

```
set switch agingtimer|ageingtimer=value
```

Parameter

agingtimer ***or*** ageingtimer	Specifies the aging timer for the MAC address table. The value is in seconds. The range is 0 to 1048575. The default is 300 seconds (5 minutes). The parameters are equivalent.

Description

This command is used to set the aging timer, which the switch uses to delete inactive dynamic MAC addresses from the MAC address table. This prevents the table from becoming full of addresses of inactive nodes. Addresses are considered inactive if no packets are sent to or received from the nodes of the addresses for the duration of the timer.

Setting the aging timer to 0 disables the timer. No dynamic MAC addresses are aged out and the table stops learning new addresses after reaching its maximum capacity.

To view the current setting for the MAC address aging timer, refer to “SHOW SWITCH AGINGTIMER|AGEINGTIMER” on page 200.

Example

The following command sets the aging timer to 120 seconds (2 minutes):

```
set switch agingtimer=120
```

AlliedWare Plus Command

Syntax

To set the aging timer for the MAC address table:

```
mac address-table ageing-time value
```

To return the aging timer to its default value:

```
no mac address-table ageing-time
```

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This command sets the aging timer to 500 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# mac address-table ageing-time 500
```

This command returns the aging timer to its default setting of 300 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no mac address-table ageing-time
```

SHOW SWITCH AGINGTIMER|AGEINGTIMER

AlliedWare Plus
Command
Available

Syntax

```
show switch agingtimer|ageingtimer
```

Parameters

None.

Description

This command displays the current setting for the aging timer. The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. To set the aging timer, refer to “SET SWITCH AGINGTIMER|AGEINGTIMER” on page 198.

Figure 38 illustrates the information displayed by this command.

```
Aging interval: 300 second(s)
```

Figure 38. SHOW SWITCH AGINGTIMER|AGEINGTIMER Command

Example

The following command displays the current setting for the MAC address aging timer:

```
show switch agingtimer
```

AlliedWare Plus Command

To view the aging timer with the AlliedWare Plus commands, refer to the AlliedWare Plus command in “SHOW SWITCH FDB” on page 201.

SHOW SWITCH FDB

AlliedWare Plus
Command
Available

Syntax

```
show switch fdb [macaddress|destaddress=macaddress]
[port=port] [type|status=static|staticunicast|
staticmulticast|dynamic|dynamicunicast|dynamicmulticast]
[vlan=name] [module=value]
```

Parameters

address
Specifies a MAC address. Use this parameter to determine the port on the switch on which a particular MAC address was learned (dynamic) or assigned (static). The address can be entered in either of the following formats:

xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

port
Specifies a port on the switch. Use this parameter to view all addresses learned on a particular port. You can specify more than one port.

type ***or*** status
Displays specific types of MAC addresses. Options are:

static
Displays all static unicast and multicast MAC addresses.

staticunicast
Displays all static unicast addresses.

staticmulticast
Displays all static multicast addresses.

dynamic
Displays all dynamic unicast and multicast MAC addresses.

dynamicunicast
Displays all dynamic unicast addresses.

dynamicmulticast
Displays all dynamic multicast addresses.

vlan
Specifies a VLAN name. Use this parameter to view the MAC addresses learned or assigned to the ports of a particular VLAN on the switch.

module
Specifies the stack ID number of a switch in an AT-9400 Stack. Use this parameter to view the MAC address table of a member switch in a stack. All the MAC address tables of the switches in the stack are the same, but you can use this option to view addresses that member switches haven't yet shared with the other units. To view the stack ID numbers, use "SHOW STACK" on page 106.

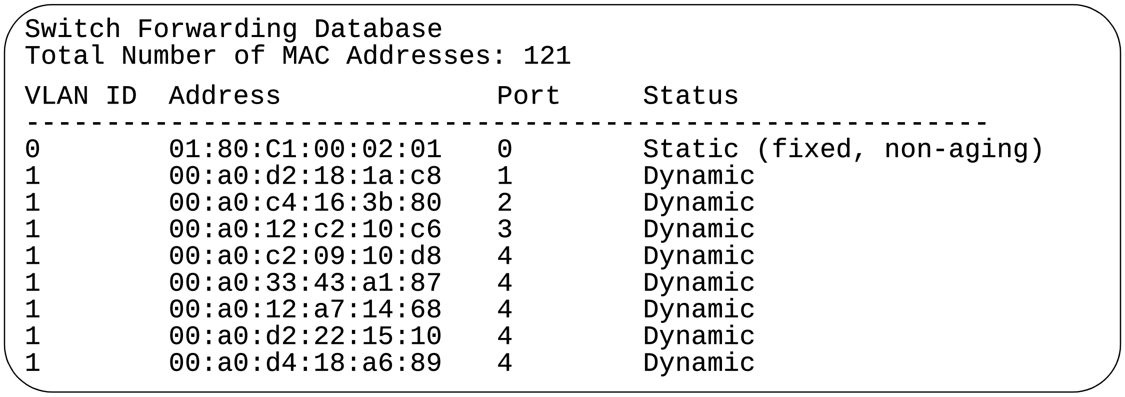
Note
You can specify more than one parameter in the command.

Description

This command displays the unicast and multicast MAC addresses learned or assigned to the ports on the switch and stored in the switch's MAC address table.

If you are managing an AT-9400 Stack, this command displays the MAC address table on the master switch. However, you can use the MODULE parameter to view the MAC address tables of member switches.

Figure 39 is an example of the information displayed by this command for unicast addresses.



```
Switch Forwarding Database
Total Number of MAC Addresses: 121

VLAN ID  Address             Port     Status
------------------------------------------------------------
0        01:80:C1:00:02:01   0        Static (fixed, non-aging)
1        00:a0:d2:18:1a:c8   1        Dynamic
1        00:a0:c4:16:3b:80   2        Dynamic
1        00:a0:12:c2:10:c6   3        Dynamic
1        00:a0:c2:09:10:d8   4        Dynamic
1        00:a0:33:43:a1:87   4        Dynamic
1        00:a0:12:a7:14:68   4        Dynamic
1        00:a0:d2:22:15:10   4        Dynamic
1        00:a0:d4:18:a6:89   4        Dynamic
```

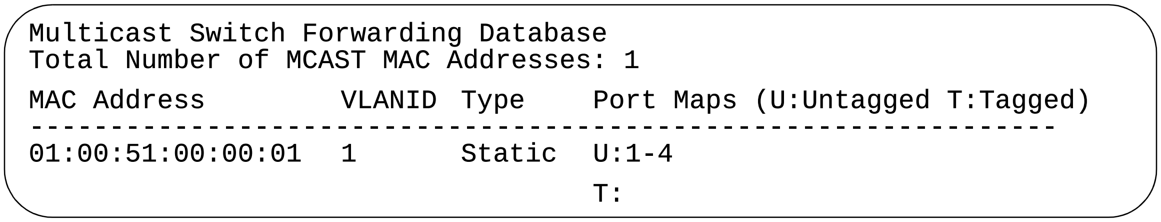
Figure 39. SHOW SWITCH FDB Command - Unicast Addresses

The first address in the unicast MAC address table is the address of the stand-alone switch. If you are managing an AT-9400 Stack, the first address is the MAC address of the master switch.

The columns are defined here:

- ❐ VLAN ID - The ID number of the VLAN where the port is an untagged member.
- ❐ Address - The dynamic or static unicast MAC address learned on or assigned to the port.
- ❐ Port - The port where the address was learned or assigned. The MAC address with port 0 is the address of the switch.
- ❐ Status - The type of address: static or dynamic.

Figure 40 is an example of a multicast address.



```
Multicast Switch Forwarding Database
Total Number of MCAST MAC Addresses: 1
MAC Address        VLANID  Type    Port Maps (U:Untagged T:Tagged)
----------------------------------------------------------------
01:00:51:00:00:01  1       Static  U:1-4
                                   T:
```

Figure 40. SHOW SWITCH FDB Command - Multicast Addresses

The columns are defined here:

- MAC Address - The static or dynamic unicast MAC address.
- VLAN ID - The ID number of the VLAN where the port is an untagged member.
- Type - The type of the address: static or dynamic.
- Port Maps - The tagged and untagged ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different groups.

Examples

The following command displays all the static and dynamic unicast MAC addresses in the switch’s MAC address table:

```
show switch fdb
```

The following command displays just the static unicast MAC addresses:

```
show switch fdb type=static
```

The following command displays the static and dynamic multicast addresses:

```
show switch fdb type=multicast
```

The following command displays just the static multicast addresses:

```
show switch fdb type=staticmulticast
```

The following command displays the port where the MAC address 00:A0:D2:18:1A:11 was learned (dynamic) or added (static):

```
show switch fdb address=00A0D2181A11
```

The following command displays the MAC addresses learned on port 2:

```
show switch fdb port=2
```

The following command displays the MAC addresses learned on the ports in the Sales VLAN:

```
show switch fdb vlan=sales
```

The following command displays the static MAC addresses on port 17:

```
show switch fdb port=17 type=static
```

The following command displays the MAC address table for a switch with the stack ID 2 in an AT-9400 Stack:

```
show switch fdb module=2
```

AlliedWare Plus Command

Syntax

```
show mac address-table
```

Modes

User Exec mode and Privileged Exec mode

Description

This command is equivalent to entering the SHOW SWITCH FDB command without any parameters. It displays all the MAC addresses in the MAC address table of a stand-alone switch or a master switch in an AT-9400 Stack. The aging timer is displayed at the bottom of the list of the MAC addresses.

Example

```
awplus# show mac address-table
```

Chapter 11

Static Port Trunking Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD SWITCH TRUNK

AlliedWare Plus Command Available

Syntax

```
add switch trunk=name [tgid=id_number] port=port
```

Parameters

trunk — Specifies the name of the static port trunk to be modified.

tgid — Specifies the ID number of the static port trunk to be modified. The range is 1 to 6. This parameter is optional.

port — Specifies the port to be added to the port trunk. You can add more than one port at a time.

Description

This command adds ports to an existing static port trunk. To initially create a static port trunk, refer to “CREATE SWITCH TRUNK” on page 208.

⚠ **Caution**

Disconnect all the network cables from the ports of the trunk on the switch before using this command. Adding a port to a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

Note

If the port you are adding will be the lowest numbered port in the trunk, its parameter settings will overwrite the settings of the existing ports in the trunk. Consequently, you check to see if its settings are appropriate prior to adding it to the trunk. If the port will not be the lowest numbered port, then its settings are changed to match the settings of the existing ports in the trunk.

Note

If the port to be added to a trunk is already a member of another static trunk, you must first remove it from its current trunk assignment. To remove ports from a trunk, see “DELETE SWITCH TRUNK” on page 212.

Example

The following command adds port 5 to a port trunk called load22:

```
add switch trunk=load22 port=5
```

AlliedWare Plus Command

The AlliedWare Plus command used to add ports to static port trunks is the same command used to create new trunks. For instructions, refer to the AlliedWare Plus command in “CREATE SWITCH TRUNK” on page 208.

CREATE SWITCH TRUNK

AlliedWare Plus Command Available

Syntax

```
create switch trunk=name port=ports
[select=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

Parameters

trunk Specifies the name of the trunk. The name can be up to 16 alphanumeric characters. No spaces or special characters are allowed.

port Specifies the ports to be added to the port trunk.

select Specifies the load distribution method. Options are:

macsrc	Source MAC address.
macdest	Destination MAC address.
macboth	Source address/destination MAC address.
ipsrc	Source IP address.
ipdest	Destination IP address.
ipboth	Source address/destination IP address.

Description

This command creates a static port trunk. To create the trunk, you specify the ports on the switch that will constitute the trunk.

Caution
Do not connect the cables to the trunk ports on the switches until after you have created the trunk in the management software. Connecting the cables before configuring the software will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Note
Before creating a static port trunk, examine the speed, duplex mode, and flow control settings of the lowest numbered port to be in the trunk. Check to be sure that the settings are correct for the end node to which the trunk will be connected. When you create the trunk, the

AT-S63 Management Software copies the settings of the lowest numbered port in the trunk to the other ports so that all the settings are the same.

You should also check to be sure that the ports are untagged members of the same VLAN. You cannot create a trunk of ports that are untagged members of different VLANs.

Note
All ports in a trunk must operate at the same speed. When you include port 23R or 24R in a trunk and the port transitions to redundant uplink status, the port speed is automatically adjusted to 1000 Mbps. If the other ports in the trunk are operating at a different speed, port trunking may be unpredictable. Because of these port speed variables, Allied Telesis suggests that you not include port 23R or 24R in a port trunk.

Note
If the ports that are to constitute the new trunk are already members of another static trunk, you must first remove them from their current trunk assignment. To remove ports from a static trunk, see “DELETE SWITCH TRUNK” on page 212.

Examples

The following command creates a static port trunk using ports 3 through 6. The command names the trunk “load22” and sets the load distribution method to destination MAC address.

```
create switch trunk=load22 port=3-6 select=macdest
```

The following command creates a port trunk consisting of ports 15,17, and 22. The command names the trunk “trunk4”. No load distribution method is specified, so the default source and destination MAC addresses method is used:

```
create switch trunk=trunk4 port=15,17,22
```

AlliedWare Plus Command

Syntax

To create a static port trunk or to add ports to an existing trunk:

```
static-channel-group ID_number
```

To change the load distribution method:

```
interface trunk_name
port-channel load-balance dst-ip|dst-mac|src-dst-ip|
src-dst-mac|src-ip|src-mac
```

Modes

To create a static port trunk or to add ports to an existing trunk:

Port Interface mode

To change the load distribution method:

Static Port Trunk Interface mode

Description

These commands are used to create new static port trunks, to add ports to existing trunks, and to change the load distribution methods of trunks. If you specify an unused trunk ID number, the command creates a new static port trunk. If the ID number is of an existing trunk, the ports are added to the designated trunk.

When you create a new static port trunk, you have to assign it an ID number, in the range of 1 to 32. This number is used to identify a trunk and to give it a name. The name, assigned automatically by the management software, consists of the prefix “sa” followed by the ID number. For instance, if you assign a new trunk the ID number 5, its name will be “sa5.”

It is important not to confuse this number with the ID number that is assigned automatically to new static port trunks that are created with the other management interfaces. That number, which is referred to as the TGID, has the same range but is completely unrelated. If, as an example, you assigned a new trunk the ID number 5 with the AlliedWare Plus command, its TGID number will be whatever the next available number happens to be. The rule is, to modify a trunk created in the AlliedWare Plus command interface, you have to specify its ID number, not its TGID number.

These commands have the following rules and restrictions:

❒ When using the STATIC-CHANNEL-GROUP command to create new trunks or to add ports to existing trunks, enter just the ID number of the new or existing trunk.

❒ When you use the INTERFACE command prior to the PORT-CHANNEL LOAD BALANCE command to change the load distribution method of trunks, you must enter the full name of a trunk, which is “sa” followed by the ID number.

❒ You cannot use the AlliedWare Plus commands to modify static port trunks created with any of the other management interfaces.

Examples

This example creates a new static port trunk of ports 11 and 12, with the ID number 2 and the load distribution method of source MAC addresses. If there is already a static port trunk with the same TGID, the commands add the ports to it:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11-12
awplus(config-if)# static-channel-group 2
awplus(config-if)# exit
awplus(config)# interface sa2
awplus(config-if)# port-channel load-balance src-mac
```

This example sets the load distribution method to destination MAC addresses for a trunk named “sa4”:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface sa4
awplus(config-if)# port-channel load-balance dst-mac
```

DELETE SWITCH TRUNK

AlliedWare Plus Command Available

Syntax

```
delete switch trunk=name port=port
```

Parameters

trunk	Specifies the name of the static port trunk to be modified.
port	Specifies the port to be removed from the existing port trunk. You can remove more than one port at a time.

Description

This command removes ports from a static port trunk. To completely remove a port trunk from a switch, see “DESTROY SWITCH TRUNK” on page 214.

Caution
Disconnect all the data cables from the ports of the trunk on the switch before using this command. Removing a port from a port trunk without first disconnecting the cables may result in loops in your network topology, which can produce broadcast storms and poor network performance.

Note
You cannot remove ports from a trunk that has only two ports because a static trunk must have a minimum of two ports.

Example

The following command removes port 9 from a port trunk called Dev_trunk:

```
delete switch trunk=Dev_trunk port=9
```

AlliedWare Plus Command

Syntax

```
no static-channel-group tgid
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is used both to remove ports from static port trunks and to delete trunks. A trunk is automatically deleted when you remove all of its ports.

Example

These commands remove ports 22 and 23 from a port trunk that has the TGID number 4. The trunk is deleted if these are the only ports in the trunk:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22-23
awplus(config-if)# no static-channel-group 4
```

DESTROY SWITCH TRUNK

AlliedWare Plus
Command
Available

Syntax

```
destroy switch trunk=name
```

Parameter

trunk	Specifies the name of the trunk to be deleted.

Description

This command deletes a static port trunk from a switch. After a port trunk has been deleted, the ports that made up the trunk can be connected to different end nodes.

Caution
Disconnect the cables from the port trunk on the switch before destroying the trunk. Deleting a port trunk without first disconnecting the cables may create loops in your network topology. Data loops may result in broadcast storms and poor network performance.

Example

The following command deletes the trunk called load22 from the switch:

```
destroy switch trunk=load22
```

AlliedWare Plus Command

The AlliedWare Plus command for deleting static port trunks is also the command for removing ports from trunks. For instructions, refer to the AlliedWare Plus command described in “DELETE SWITCH TRUNK” on page 212.

SET SWITCH TRUNK

AlliedWare Plus
Command
Available

Syntax

```
set switch trunk=name
select=macsrc|macdest|macboth|ipsrc|ipdest|ipboth
```

Parameters

trunk — Specifies the name of the static port trunk.

select — Specifies the load distribution method. Options are:

macsrc	Source MAC address.
macdest	Destination MAC address.
macboth	Source address/destination MAC address.
ipsrc	Source IP address.
ipdest	Destination IP address.
ipboth	Source address/destination IP address.

Description

This command is used to change the load distribution methods of existing static port trunks.

Example

The following command changes the load distribution method to source MAC address for a trunk named “Load11”:

```
set switch trunk=Load11 select=macsrc
```

AlliedWare Plus Command

Syntax

```
interface trunk_name
port-channel load-balance dst-ip|dst-mac|src-dst-ip|
src-dst-mac|src-ip|src-mac
```

Mode

Static Port Trunk Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example sets the load distribution method to source MAC addresses for a trunk named “sa1”:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface sa1
awplus(config-if)# port-channel load-balance src-mac
```

SHOW SWITCH TRUNK

AlliedWare Plus Command Available

Syntax

```
show switch trunk
```

Parameters

None.

Description

This command displays the names, ports, and load distribution methods of the static port trunks on the switch. An example of the command is shown in Figure 41.

```
Trunk group ID ............ 2
   Trunk status ........... UP
   Trunk group name ....... Server11
   Trunk method ........... SRC/DST MAC
   Ports .................. 12-16
```

Figure 41. SHOW SWITCH TRUNK Command

The command displays the following information:

- Trunk group ID - The ID number of the static port trunk.
- Trunk status - The operational status of the trunk. If the trunk has established a link with the other device, status will be UP. If the trunk has not establish a link or the ports in the trunk are disabled, status will be DOWN.
- Trunk group name - The name of the static port trunk.
- Trunk method - One of the following load distribution methods:

SRC MAC	Source MAC address.
DST MAC	Destination MAC address.
SRC/DST MAC	Source address/destination MAC address.
SRC IP	Source IP address.
DST IP	Destination IP address.
SRC/DST IP	Source address/destination IP address.

- Ports - The ports of the static port trunk.

Example

```
show switch trunk
```

AlliedWare Plus Command

Syntax

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

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show static-channel-group
```

Chapter 12
LACP Port Trunking Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD LACP PORT

AlliedWare Plus
Command
Available

Syntax

```
add lacp aggregator=name port=port
```

Parameters

aggregator — Specifies the name of the aggregator. The name is case-sensitive.

port — Specifies the port to add to the aggregator. You can add more than one port at a time.

Description

This command adds ports to an existing aggregator. You must identify the aggregator by its name. To display the names of the aggregators on the switch, refer to “SHOW LACP” on page 233. To create an aggregator, refer to “CREATE LACP AGGREGATOR” on page 222.

Review the following before adding a port to an aggregator:

- Verify that the port’s speed is set to Auto-Negotiation or 100 Mbps, full-duplex. Aggregate trunks do not support half-duplex mode.
- The ports of an aggregator must be untagged ports of the same VLAN.
- You cannot add a port to an aggregator that is below the lowest numbered port in the aggregator, also referred to as the base port. For example, if an aggregator consists of ports 7 to 12, you cannot add ports 1 to 6. To change the base port of an aggregator, you must delete and recreate the aggregator.

Caution
A network cable should not be connected to a port on the switch until after the port is added to the aggregator. Connecting the cable before the port is a part of an aggregator can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Examples

The following command adds ports 8 and 22 to an aggregator named “agg_1”:

```
add lacp aggregator=agg_1 port=8,22
```

AlliedWare Plus Command

Syntax

```
channel-group integer
```

Mode

Port Interface mode

Description

This command is used to create new aggregators and to add ports to existing aggregators. This differs from the standard command line interface which has different commands for these two functions.

If you specify an unused name, the command creates a new aggregator. If, on the other hand, you specify the name of an existing aggregator, the designated ports are added to the aggregator.

This command does not let you specify the name, adminkey, or load distribution method of a new aggregator. The default values are used for these parameters.

If you use this command to create the first aggregator on a switch, LACP is automatically activated. You do not have to activate it manually.

Example

These commands create a new aggregator of ports 11 and 12, named ‘po2’. LACP is automatically activated if this is the first aggregator on the switch. If there is already an aggregator with the same name, the command adds the ports to it:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11-12
awplus(config-if)# channel-group 2
```

CREATE LACP AGGREGATOR

AlliedWare Plus
Command
Available

Syntax

```
create lacp aggregator=name|adminkey=0xkey port=port
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

Parameters

aggregator — Specifies a name for the new aggregator. The name can be up to 20 alphanumeric characters. No spaces or special characters are allowed. If no name is specified, the default name is DEFAULT_AGG followed by a number.

adminkey — Specifies an adminkey number for the aggregator. This is a hexadecimal number in the range of 0x1 to 0xffff. If this parameter is omitted, the default adminkey of the lowest numbered port in the aggregator is used.

port — Specifies the ports of the aggregator.

distribution — Specifies the load distribution method, which can be one of the following:

macsrc	Source MAC address.
macdest	Destination MAC address.
macboth	Source and destination MAC addresses. This is the default.
ipsrc	Source IP address.
ipdest	Destination IP address.
ipboth	Source and destination IP addresses.

If this parameter is omitted, the source and destination MAC addresses load distributed method is selected by default.

Description

This command creates an LACP aggregator. Note the following when creating a new aggregator:

❒ You can specify either a name or an adminkey but not both when creating a new aggregator.

- When you create a new aggregator by specifying a name, the adminkey is based on the operator key of the lowest numbered port in the aggregator.
- When you create an aggregator by specifying an adminkey, the aggregator’s default name is DEFAULT_AGG followed by the port number of the lowest numbered port in the aggregator. For instance, an aggregator of ports 12 to 16 is given the name DEFAULT_AGG12.
- Before creating an aggregator, you should verify that the ports that will be members of the aggregator are set to Auto-Negotiation or 100 Mbps, full-duplex. Aggregate trunks do not support half-duplex mode.
- All the ports of an aggregator must be untagged ports of the same VLAN.
- You cannot change the name or adminkey of an existing aggregator. That function requires deleting the aggregator and recreating it.

⚠ **Caution**

Do not connect the cables to the ports of the aggregator on the switch until after you have configured LACP and the aggregators on both devices that will be interconnected by the trunk. Connecting the cables before configuring the aggregators and activating the protocol will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Examples

The following command creates an LACP aggregator named “sw_agg_1” of ports 1 through 4. The load distribution method is source MAC address. Since the aggregator is being created by name, the default operator key for port 1, the lowest numbered port in the aggregator, becomes the adminkey:

```
create lacp aggregator=sw_agg_1 port=1-4 distribution=macsrc
```

The following command creates an LACP aggregator of ports 10, 12, 15 to 18 with an adminkey number of 0x7A. The default name for the aggregator is DEFAULT_AGG10 because the command specifies an adminkey and because port 10 is the lowest numbered port in the aggregator. Since no load distribution method is specified, the source and destination MAC addresses load distributed method is used by default:

```
create lacp adminkey=0x7A port=10,12,15-18
```

AlliedWare Plus Command

To create a new aggregator with the AlliedWare Plus commands, use the CHANNEL-GROUP command in the AlliedWare Plus Command section in “ADD LACP PORT” on page 220. The same command is used both to create new aggregators and to add ports to existing aggregators.

DELETE LACP PORT

AlliedWare Plus Command Available

Syntax

```
delete lacp aggregator=name port=port
```

Parameters

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
port	Specifies the port to delete from an aggregator. You can delete more than one port at a time.

Description

This command removes a port from an aggregator. You must identify the aggregator by its name. To display the names of the aggregators on the switch, refer to “SHOW LACP” on page 233. To completely remove an aggregator, see “DESTROY LACP AGGREGATOR” on page 226.

⚠ **Caution**
Disconnect the network cable from a port before removing it from an aggregator. Removing a port without first disconnecting the cable can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Note
You cannot delete the lowest numbered port from an aggregator, also referred to as the base port. For example, if an aggregator consists of ports 7 to 12, you cannot delete port 7. You must delete and recreate an aggregator to remove the base port.

Example

The following command removes port 9 from the “lacp_server” aggregator:

```
delete lacp aggregator=lacp_server port=9
```

AlliedWare Plus Command

Syntax

```
no channel-group integer
```

Mode

Port Interface mode

Description

This command is used to remove ports from the aggregators and to delete the aggregators. You delete an aggregator by deleting all of its ports This differs from the other command line interface where there are different commands for removing ports and for deleting aggregators.

Deleting the last aggregator on a switch deactivates LACP.

Example

These commands delete ports 11 and 12 from an aggregator named ‘po2’. The aggregator is deleted if these are its only ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11-12
awplus(config-if)# no channel-group 2
```

DESTROY LACP AGGREGATOR

AlliedWare Plus Command Available

Syntax

```
destroy lacp aggregator=name|adminkey=0xkey
```

Parameter

aggregator	Specifies the name of the aggregator. The name is case-sensitive.
adminkey	Specifies the adminkey number of the aggregator. This is a hexadecimal number between 0x1 and 0xffff.

Description

This command deletes an LACP aggregator from the switch. You can identify the aggregator by its name or adminkey number. To display the names and adminkeys of the aggregators on the switch, refer to “SHOW LACP” on page 233.

Caution
Disconnect the network cables from the ports of the aggregator before performing this command. Deleting the aggregator without first disconnecting the cables can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Example

The following command deletes an aggregator named “agg_15”:

```
destroy lacp aggregator=agg_15
```

The following command deletes an aggregator with an adminkey number of 0x1A:

```
destroy lacp adminkey=0x1a
```

AlliedWare Plus Command

To delete an aggregator using the AlliedWare Plus commands, delete all of the aggregator’s ports with the NO CHANNEL-GROUP command described in “DELETE LACP PORT” on page 224.

DISABLE LACP

AlliedWare Plus Command Available

Syntax

```
disable lacp
```

Parameters

None.

Description

This command disables LACP on the switch. The default is disabled.

⚠ **Caution**
Do not disable LACP if there are defined aggregators without first disconnecting all cables connected to the aggregate trunk ports. Otherwise, a network loop may occur, resulting in a broadcast storm and poor network performance.

Example

The following command disables LACP on the switch:

```
disable lacp
```

Equivalent Command

```
set lacp state=disable
```

For information, see "SET LACP STATE" on page 232.

AlliedWare Plus Command

There is no separate AlliedWare Plus command for disabling LACP. LACP is automatically disabled when you delete the last aggregator on the switch with the NO CHANNEL-GROUP command, described in AlliedWare Plus Command section in "DELETE LACP PORT" on page 224.

ENABLE LACP

AlliedWare Plus
Command
Available

Syntax

```
enable lacp
```

Parameters

None.

Description

This command activates LACP on the switch. The default is disabled.

Example

The following command activates LACP:

```
enable lacp
```

Equivalent Command

```
set lacp state=enable
```

For information, see “SET LACP STATE” on page 232.

AlliedWare Plus Command

The AlliedWare Plus command interface does not have a separate command to enable LACP. LACP is automatically enabled when you use the CHANNEL-GROUP command and create the first aggregator on the switch. For instructions, refer to the AlliedWare Plus command in “ADD LACP PORT” on page 220.

SET LACP AGGREGATOR

Syntax

```
set lacp aggregator=name|adminkey=key
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|ipboth]
```

Parameters

aggregator Specifies the name of the aggregator you want to modify. The name is case-sensitive.

adminkey Specifies the adminkey number of the aggregator you want to modify. This is a hexadecimal number between 0x1 and 0xffff.

distribution Specifies one of the following load distribution methods:

macsrc	Source MAC address.
macdest	Destination MAC address.
macboth	Source address/destination MAC address. This is the default.
ipsrc	Source IP address.
ipdest	Destination IP address.
ipboth	Source address/destination IP address.

Description

This command modifies the load distribution method of an existing LACP aggregator. You can identify the aggregator by its name or adminkey. To display the names and adminkeys of the aggregators on the switch, refer to "SHOW LACP" on page 233.

Note
You cannot change the name or adminkey of an existing aggregator.

Examples

The following command changes the load distribution method of an LACP aggregator titled "agg_5" to the source MAC address method:

```
set lacp aggregator=agg_5 distribution=macsrc
```

The following command changes the load distribution method of an LACP aggregator with the adminkey 0x22 to the destination MAC address method:

```
set lacp adminkey=0x22 distribution=macdest
```

SET LACP SYSPRIORITY

Syntax

```
set lacp syspriority=0xpriority
```

Parameters

syspriority	Specifies the LACP system priority value for a switch. This is a hexadecimal value from 0x1 to 0xffff. The lower the number, the higher the priority. The default is 0x0080.

Description

This command sets the LACP priority of the switch. LACP uses the priority to resolve conflicts between two switches to decide which switch makes the decision about which ports to aggregate.

Example

The following command sets the LACP priority on the switch to 0x8000:

```
set lacp syspriority=0x8000
```

SET LACP STATE

AlliedWare Plus Command Available

Syntax

```
set lacp state=enable|disable
```

Parameters

state	Specifies the state of LACP on the switch. The options are:	
	enable	Enables LACP.
	disable	Disables LACP. This is the default.

Description

This command is used to enable or disable LACP on the switch.

⚠ **Caution**
If there are aggregators defined on the switch, do not disable LACP until you have disconnected all the cables from the aggregate trunk ports. Otherwise, a network loop might occur, resulting in a broadcast storm and poor network performance.

Example

The following command activates LACP on the system:

```
set lacp state=enable
```

Equivalent Commands

```
disable lacp
```

For information, see “DISABLE LACP” on page 227.

```
enable lacp
```

For information, see “ENABLE LACP” on page 228.

AlliedWare Plus Command

The AlliedWare Plus interface does not have a separate command to enable or disable LACP on the switch. LACP is automatically enabled when you create the first aggregator and disabled when you delete the last aggregator. For instructions, refer to the AlliedWare Plus commands in “ADD LACP PORT” on page 220 and “DELETE LACP PORT” on page 224.

SHOW LACP

AlliedWare Plus Command Available

Syntax

```
show lacp [port=port] [aggregator] [machine=port]
```

Parameter

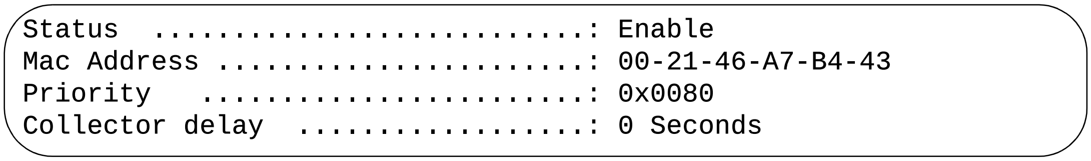
port Specifies the port(s) to display.

aggregator Displays information about the aggregators.

machine Specifies the LACP machine state for a port or ports on the system.

Description

This command is used to display the configuration and/or machine states of the ports, and/or the aggregators. Entering the command without any parameters displays general LACP status information. Figure 42 illustrates the information.



```
Status  ..........................: Enable
Mac Address ......................: 00-21-46-A7-B4-43
Priority   .......................: 0x0080
Collector delay  .................: 0 Seconds
```

Figure 42. SHOW LACP Command

The command displays the following information:

- Status - Whether the LACP protocol is enabled or disabled on the switch.
- MAC Address - The MAC address of the switch.
- Priority - The LACP system priority value assigned to the switch.

The PORT parameter displays LACP port information. Figure 43 on page 234 illustrates the information displayed by this parameter. For definitions, refer to the IEEE 802.3ad standard.

```
Port ............. 05
Aggregator ....... LACP sw22
ACTOR                               PARTNER
============================================
Actor Port ............. 05         Partner Port ......... 00
Selected ............... SELECTED   Partner System ....... 00-30-84-AB-EF-CD
Oper Key ............... 0xf705     Oper Key  ............ 0xff07
Oper Port Priority  .... 0x0005     Oper Port Priority ... 0x0007
Individual ............. NO         Individual ........... NO
Synchronized............ YES        Synchronized.......... YES
Collecting  ............ YES        Collecting ........... YES
Distributing ........... YES        Distributing ......... YES
Defaulted .............. NO         Defaulted ............ NO
Expired ................ NO         Expired .............. NO
Actor Churn   .......... YES        Partner Churn ........ YES
```

Figure 43. SHOW LACP Command with the PORT Parameter

The AGGREGATOR parameter displays information about each existing aggregator. Figure 44 illustrates the information displayed by this parameter.

```
Aggregator # 1 ..... DEFAULT_AGG5
Admin Key .......... 0x0001
Oper Key ........... 0x0045
Speed .............. 1000 Mbps
Distribution Mode .. MACBoth
Ports configured ... 5-8
Ports in LAGID...... 5-8
Aggregated Port .... 5-8
```

Figure 44. SHOW LACP Command with the AGGREGATOR Parameter

Examples

The following command displays general LACP status information:

```
show lacp
```

The following command displays the LACP configuration for ports 13 and 16:

```
show lacp port=13,16
```

The following command displays the configuration of the aggregators on the system:

```
show lacp aggregator
```

The following command displays the LACP machine states for each port on the system:

```
show lacp machine
```

AlliedWare Plus Command

Syntax

```
show etherchannel
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays a combination of the information of the SHOW LACP command without the optional parameters and the information from the AGGREGRATOR parameter.

Example

```
awplus# show etherchannel
```

Chapter 13

Port Mirroring Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

SET SWITCH MIRROR

AlliedWare Plus Command Available

Syntax

```
set switch mirror=port
```

Parameter

mirror Specifies the destination port for the port mirror. This is the port where the traffic from the source ports is copied. You can specify only one port as the destination port. Specifying “0” (zero) stops port mirroring so that the destination port can again be used as a normal networking port.

Description

This command enables mirroring and specifies the destination port, or stops port mirroring. To select the source ports, refer to “SET SWITCH PORT MIRROR” on page 239.

Examples

The following command enables mirroring and makes port 11 the destination port:

```
set switch mirror=11
```

The following command stops port mirroring:

```
set switch mirror=0
```

AlliedWare Plus Command

The AlliedWare Plus command for designating the destination port of a port mirror is also the command for specifying the source ports. For information, refer to the AlliedWare Plus command in “SET SWITCH PORT MIRROR” on page 239.

SET SWITCH PORT MIRROR

AlliedWare Plus
Command
Available

Syntax

```
set switch port=port mirror=none|rx|tx|both
```

Parameters

port — Specifies a source port of a port mirror. You can specify more than one port. For instructions, refer to "Port Numbers in Commands" on page 48.

mirror — Specifies the traffic on the source ports to be mirrored to the destination port. The options are:

- rx — Specifies ingress mirroring.
- tx — Specifies egress mirroring.
- both — Specifies both ingress and egress mirroring.
- none — Removes a port as a source port.

Description

This command specifies the source ports of a port mirror. If the port mirror already has source ports, the new source ports are added to the existing ports. You can also use the command to remove source ports.

You must set the destination port before you can select the source ports. To set the destination port, refer to "SET SWITCH MIRROR" on page 238.

Examples

The following command specifies ports 16 and 17 as new source ports for the port mirror. Only the ingress traffic is mirrored:

```
set switch port=16-17 mirror=rx
```

The following command removes ports 5, 7, and 10 as source ports of a port mirror:

```
set switch port=5,7,10 mirror=none
```

AlliedWare Plus Command

Syntax

To create a port mirror or to add ports to an existing port mirror:

```
interface destination_port
mirror interface source_ports direction
receive|transmit|both
```

To remove ports from a port mirror or to disable port mirroring:

```
interface source_ports
no mirror interface
```

Mode

Port Interface mode

Description

To stop port mirroring with the AlliedWare Plus commands and to return the destination port to normal network operations, remove all of the source ports.

Examples

This example creates a port mirror that copies the ingress traffic on port 3, the source port, to port 5, the destination port. If port 5 is already acting as a destination port of a port mirror, these commands add port 3 to the port mirror:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5
awplus(config-if)# mirror interface 3 direction receive
```

These commands remove ports 7 and 8 from the port mirror. If these are the only source ports in the mirror, the port mirror is disabled and the destination port resumes normal network operations

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 7,8
awplus(config-if)# no mirror interface
```

SHOW SWITCH MIRROR

AlliedWare Plus
Command
Available

Syntax

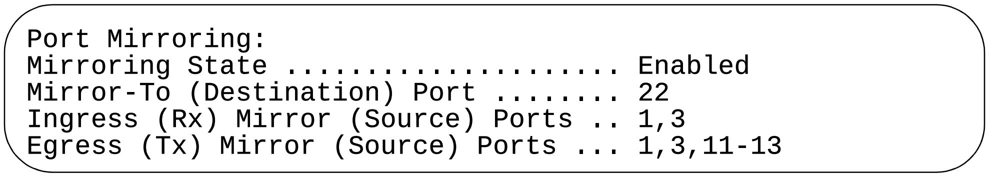
```
show switch mirror
```

Parameters

None.

Description

This command displays the source and destination ports of the port mirror on the switch. An example is shown in Figure 45.



```
Port Mirroring:
Mirroring State ..................... Enabled
Mirror-To (Destination) Port ........ 22
Ingress (Rx) Mirror (Source) Ports .. 1,3
Egress (Tx) Mirror (Source) Ports ... 1,3,11-13
```

Figure 45. SHOW SWITCH MIRROR Command

The command provides the following information about the port mirror:

- Mirroring State - The port mirroring status, Enabled or Disabled. If port mirroring is disabled on the switch, only this line is displayed by the command.
- Mirror-To (Destination) Port - The port functioning as the destination port.
- Ingress (Rx) Mirror (Source) Port - The port(s) whose ingress (received) traffic is mirrored.
- Egress (Tx) Mirror (Source) Port - The port(s) whose egress (transmitted) traffic is mirrored.

Example

The following command displays the status and the ports of the port mirror:

```
show switch mirror
```

AlliedWare Plus Command

Syntax

```
show mirror
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the same information as the standard command, but in a different format. Here is an example. The Mirror Test Port is the destination port of the port mirror. The Monitored Ports are the source ports.

```
awplus# show mirror
Mirror Test Port Name: port1.22
Mirror option: Enabled
Monitored Port Name: port1.1
Mirror direction: receive
Monitored Port Name: port1.3
Mirror direction: receive
Monitored Port Name: port1.1
Mirror direction: transmit
Monitored Port Name: port1.3
Mirror direction: transmit
Monitored Port Name: port1.11
Mirror direction: transmit
Monitored Port Name: port1.13
Mirror direction: transmit
awplus#
```

Figure 46. SHOW MIRROR Command

Example

```
awplus# show mirror
```

Chapter 14

Link-flap Protection Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD LINK-FLAP

AlliedWare Plus
Command
Available

Syntax

```
add link-flap port=port|all
```

Parameters

port — Specifies a port for link-flap protection. You can configure more than one port at a time with this command. To specify all of the ports, use the ALL option.

Description

This command is used to designate ports for link-flap protection. If ports have already been designated for link-flap protection, this command adds the new ports to the existing ports. If you want to remove the existing ports while designating new ports, use the ENABLE LINK-FLAP command instead. For instructions, refer to “ENABLE LINK-FLAP” on page 248.

The status of link-flap protection on the switch is not changed by this command. If it is disabled, it remains disabled. If it is enabled, it remains enabled. To disable or enable link-flap protection with the standard commands, refer to “DISABLE LINK-FLAP” on page 247 and “ENABLE LINK-FLAP” on page 248, respectively.

Example

This example adds link-flap protection to ports 15 and 22:

```
add link-flap port=15,22
```

AlliedWare Plus Command

Syntax

```
link-flap protection
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is used like the standard command to add ports for link-flap protection. It differs from the standard command in that if link-flap protection on the switch is disabled, it enables it.

Example

This example adds link-flap protection to ports 11 to15. If link-flap protection is disabled on the switch, this command also activates it:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11-15
awplus(config-if)# link-flap protection
```

DELETE LINK-FLAP

AlliedWare Plus
Command
Available

Syntax

```
delete link-flap port=port|all
```

Parameters

port

Specifies a port to remove link-flap protection. You can remove more than one port at a time with this command. To remove all of the ports from the feature, use the ALL option.

Description

This command is used to remove link-flap protection from ports.

Example

This example removes link-flap protection from ports 15 to 17:

```
delete link-flap port=15-17
```

AlliedWare Plus Command

Syntax

```
no link-flap protection
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is used like the standard command to remove link-flap protection from ports. It differs in that it disables link-flap protection on the switch if you remove all of the ports assigned to the feature.

Example

This example removes link-flap protection from ports 18 and 24. It disables the feature if these are the only two ports assigned to the feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18,24
awplus(config-if)# no link-flap protection
```

DISABLE LINK-FLAP

AlliedWare Plus Command Available

Syntax

```
disable link-flap
```

Parameters

None.

Description

This command is used to disable link-flap protection on the switch. This is the default setting.

Example

```
disable link-flap
```

AlliedWare Plus Command

To disable link-flap protection with the AlliedWare Plus commands, use the NO LINK-FLAP PROTECTION command and remove all of the ports from the feature. For instructions, refer to the AlliedWare Plus command in "DELETE LINK-FLAP" on page 246.

ENABLE LINK-FLAP

AlliedWare Plus Command Available

Syntax

```
enable link-flap [port=port|all]
```

Parameter

port	Specifies the port on which link-flap protection is to be enabled. You can configure more than one port at a time with this command. To specify all of the ports, enter the ALL option.

Description

This command is used to activate link-flap protection on the switch. This feature protects the switch from unreliable or fluctuating links. The switch disables a port if a link fluctuates up and down a set number of times within a defined time period. A disabled port remains disabled until you enable it again with the management software.

This command is also used to add ports to link-flap protection. This command is different from the ADD LINK-FLAP command in that the ports designated in this command replace any ports already assigned to this feature, and it activates the feature if it is disabled.

Examples

This command activates link-flap protection on the switch:

```
enable link-flap
```

This command adds link-flap protection to ports 12 to 17. If ports have already been designated for the feature, these ports replace the existing ports:

```
enable link-flap port=12-17
```

AlliedWare Plus Command

To enable link-flap protection and to add ports to this feature with the AlliedWare Plus commands, use the LINK-FLAP PROTECTION command. For instructions, refer to the AlliedWare Plus command in “ADD LINK-FLAP” on page 244.

SET LINK-FLAP

AlliedWare Plus Command Available

Syntax

```
set link-flap rate=rate duration=duration
```

Parameter

rate	Specifies the number of link changes that constitute a link flap event on a port. The range is 4 to 65535 changes. The default is 10 changes.
duration	Specifies the time period in which the changes must occur to constitute a link flap event. The range is 20 to 65535 seconds. The default is 60 seconds.

Description

This command is used to establish the rate and duration of link-flap events on the ports on the switch. The rate defines the number of link changes of link-flap events. A link change is defined as anytime a port loses a link to an end node or establishes a link to an end node. The duration is the time period in which the changes must occur. At the default values, a link-flap event occurs on a port when a link experiences 10 changes within 60 seconds. As an example, if you set the rate to five changes and the duration to 120 seconds, a link flap-event occurs if a port's link changes five times within two minutes.

Example

This command sets the rate to seven changes and the duration to two minutes:

```
set link-flap rate=7 duration=120
```

AlliedWare Plus Command

Syntax

```
link-flap rate rate
```

```
link-flap duration duration
```

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This example set the rate to eight status changes and the duration to three minutes:

```
awplus> enable
awplus# configure terminal
awplus(config)# link-flap rate 8
awplus(config)# link-flap duration 180
```

SHOW LINK-FLAP

AlliedWare Plus
Command
Available

Syntax

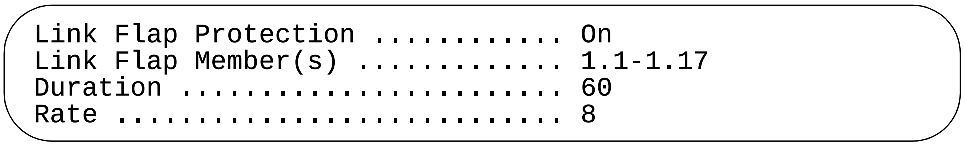
```
show link-flap
```

Parameter

None.

Description

This command displays the status of link-flap protection on the switch, the ports of the feature, and the configuration settings. Here is an example of the information this command displays.



```
Link Flap Protection ............ On
Link Flap Member(s) ............. 1.1-1.17
Duration ........................ 60
Rate ............................ 8
```

Figure 47. SHOW LINK-FLAP Command

Example

```
show link-flap
```

AlliedWare Plus Command

Syntax

```
show link-flap
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show link-flap
```

Section II

Advanced Operations

This section contains the following chapters:

Chapter 15

File System Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

COPY

AlliedWare Plus
Command
Available

Syntax

```
copy [cflash:]sourcefile.ext [cflash:]destinationfile.ext
```

Parameters

sourcefile.ext Specifies the name of the source file. If the file is stored on a compact memory flash card, precede the name with “cflash:”. If the filename contains spaces, enclose it in double quotes. Otherwise, the quotes are optional.

destinationfile.ext Specifies the name of the destination file. To store the copy on a compact memory flash card, precede the name with “cflash:”. If the filename contains spaces, enclose in double quotes. Otherwise, the quotes are optional.

Description

This command creates a copy of an existing file. It also copies files between the switch’s file system and a compact flash memory card, for those switches that support the card.

Note the following before using this command:

- This command does not accept a directory path. When copying a file to or from a compact flash card, you must first change to the appropriate directory on the card. For instructions, refer to “SET CFLASH DIR” on page 265. The default location is the root of the flash card.
- Files with the extension UKF are encryption key pairs. These files cannot be copied, renamed, or deleted from the file system.
- The new filename must be a valid filename from 1 to 16 alphanumeric characters. The name of the copy must be unique from the other files in the file system.
- *ext* is the three-letter file extension, and can be any of the types listed in Table 4. You must give the copy the same extension as the original file.

Table 4. File Extensions and File Types

Extension	File Type
.cfg	Configuration file

Table 4. File Extensions and File Types

Extension	File Type
.cer	Certificate file
.csr	Certificate enrollment request
.key	Public encryption key
.log	Event log

Examples

This command creates a copy of the configuration file “admin.cfg” in the switch’s file system and names the copy “admin2.cfg”:

```
copy admin.cfg admin2.cfg
```

This command creates a copy of the configuration file “switch 12.cfg” in the file system and names the copy “backup.cfg”:

```
copy "switch 12.cfg" backup.cfg
```

This command copies the configuration file “9408switches.cfg” from the switch’s file system to a compact flash card:

```
copy 9408switches.cfg cflash:9408switches.cfg
```

This command copies the configuration file “sales sw12.cfg” from a compact flash card to the switch’s file system and renames the file “presales_4.cfg”:

```
copy cflash:”sales sw12.cfg” presales_4.cfg
```

AlliedWare Plus Command

Syntax

```
cp [cflash:]sourcefile.ext [cflash:]destinationfile.ext
```

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command, except it does not accept spaces in the filenames.

Example

This command creates a copy of the configuration file “unit12.cfg” in the switch’s file system and names the copy “unit24.cfg”:

```
awplus# cp unit12.cfg unit24.cfg
```

This command copies the configuration file “9408switches.cfg” from the switch’s file system to a compact flash card:

```
awplus# cp 9408switches.cfg cflash:9408switches.cfg
```

This command copies the configuration file “sw12.cfg” from a compact flash card to the switch’s file system and renames the file “presales_4.cfg”:

```
awplus# cp cflash:sw12.cfg presales_4.cfg
```

CREATE CONFIG

Syntax

```
create config=[cflash:]filename.cfg
```

Parameter

config — Specifies the name of a new configuration file. If the filename contains spaces, enclose it in double quotes. Otherwise, the quotes are optional. To store the configuration file on a flash memory card, precede the name with “cflash:”.

Description

This command creates a new configuration file. The file contains the commands necessary to recreate the current configuration of the switch.

The CONFIG parameter specifies the name for the configuration file. The file extension must be “.cfg”. If the file already exists, it is replaced. If the file does not exist it is created.

The filename can be from 1 to 16 alphanumeric characters, not including the “.cfg” extension. Spaces are allowed. Be sure to enclose the name in double quotes if you include a space in the name. Wildcards are not allowed.

This command does not change the assignment of the active boot configuration file, which is the file the switch uses to configure itself the next time it is reset or power cycled. To change the active boot configuration file, refer to “SET CONFIG” on page 266.

Examples

The following command creates the new configuration file Switch12.cfg in the switch’s file system. The file will contain all of the commands necessary to recreate the switch’s current configuration:

```
create config=Switch12.cfg
```

The following command creates a configuration file named “l2 switches.cfg” and stores it on a compact flash card:

```
create config=cflash:”l2 switches.cfg”
```

DELETE FILE

AlliedWare Plus
Command
Available

Syntax

```
delete file=[cflash:]filename
```

Parameter

file

Specifies the name of the file to be deleted. A name with spaces must be enclosed in double quotes. Otherwise, the quotes are optional. If the file is stored on a compact memory flash card, precede the name with “cflash:”.

Description

This command deletes a file from the file system or from a compact flash memory card.

Note the following before using this command:

- Deleting the configuration file that is acting as the active boot configuration file causes the switch to use its default settings the next time you reboot or power cycle the switch, unless you select another active boot configuration file. For instructions on how to change the active boot configuration file, refer to see “SET CONFIG” on page 266.
- To delete a PKI certificate, you must first remove the certificate from the certificate database using “DELETE PKI CERTIFICATE” on page 861.
- This command does not accept a directory path. To delete a file on a compact flash card, you must first change to the directory where the file is stored. For instructions, refer to “SET CFLASH DIR” on page 265.
- Files with a “.ukf” extension cannot be deleted with this command. These files are encryption key pairs. To delete an encryption key pair from the switch, refer to “DESTROY ENCO KEY” on page 850.

To list the files in the file system, refer to “SHOW FILE” on page 272.

Examples

The following command deletes the certificate enrollment request SW55a.csr:

```
delete file=SW55a.csr
```

The following command deletes the configuration file named “Switch 12.cfg” from a compact flash card:

```
delete file=cflash:"Switch 12.cfg"
```

AlliedWare Plus Command

Syntax

rm [cflash:]*filename.ext*

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command, except it does not accept spaces in the filenames.

Example

This command deletes the configuration file “unit12.cfg”:

```
awplus# rm unit12.cfg
```

This command deletes the configuration file “9408switches.cfg” from a compact flash card:

```
awplus# rm cflash:9408switches.cfg
```

FORMAT DEVICE

AlliedWare Plus Command Available

Syntax

```
format device=flash
```

Parameter

device Specifies the device to format. The only option is “Flash” for the switch’s file system.

Description

This command formats the flash memory in the switch.

⚠ **Caution**
This command deletes ALL of the files in the switch’s flash memory, including the active configuration file, encryption keys, and certificates. Only the image file of the AT-S63 Management Software in the application block is retained.

⚠ **Caution**
This procedure causes a system reset. Some network traffic may be lost while the switch initializes the AT-S63 Management Software.

Example

The following example formats the flash memory in the switch:

```
format device=flash
```

AlliedWare Plus Command

Syntax

```
clear flash
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# clear flash
```

RENAME

AlliedWare Plus
Command
Available

Syntax

```
rename [cflash:]filename1.ext [cflash:]filename2.ext
```

Parameters

filename1.ext

Specifies the name of the file to be renamed. If the name contains spaces, enclose it in double quotes. Otherwise, the quotes are optional. If the file is stored on a compact memory card, precede the name with “cflash:”.

filename2.ext

Specifies the new name for the file. The filename can be from 1 to 16 alphanumeric characters, not including the filename extension. Spaces are allowed. If the name contains spaces, it must be enclosed in double quotes. The filename extension must be the same as in the original filename. The new name must be unique in the file system. If the file is stored on a compact memory card, precede the name with “cflash:”.

Description

This command renames a file in a switch’s file system or on a compact flash memory card. The source and destination file extensions must be the same.

Note the following before using this command:

- Files with the extension UKF are encryption key pairs. These files cannot be copied, renamed, or deleted from the file system.
- Renaming the active boot configuration file and then resetting the switch returns the unit to its default parameter settings, unless you save the current configuration or select another active boot configuration file. For instructions on how to change the active boot configuration file, see “SET CONFIG” on page 266.
- The command does not accept a directory path. To rename a file on a compact flash card, you must first change to the directory where the file is stored. For instructions, refer to “SET CFLASH DIR” on page 265.
- The source and destination locations must be the same.

Examples

The following command renames the file “Switch12.cfg” in the switch’s file system to “Sw 44a.cfg”:

```
rename Switch12.cfg "Sw 44a.cfg"
```

This command renames the file “sales_sw.cfg” on a flash memory card to “sales sw5.cfg”:

```
rename cflash:sales_sw.cfg cflash:”sales sw5.cfg”
```

AlliedWare Plus Command

Syntax

```
move filename1.ext filename2.ext
```

Mode

Privileged Exec mode

Description

This command has the following restrictions:

❐ It does not accept spaces in the filenames.

❐ You cannot use it to rename files on flash memory cards.

Example

This example renames the file “sw12.cfg” to sw_rm102.cfg:”

```
awplus# move sw12.cfg sw_rm102.cfg
```

SET CFLASH DIR

Syntax

```
set cflash dir=directory
```

Parameter

dir	Specifies the directory path.

Description

This command changes the current directory on the compact flash card.

Note
You cannot create directories on a compact flash card from the AT-S63 Management Software.

Example

The following command changes the current directory on a compact flash card to “configs”:

```
set cflash dir=configs
```

This command changes the current directory back to the root on the compact flash card:

```
set cflash dir=\
```

SET CONFIG

AlliedWare Plus
Command
Available

Syntax

```
set config=[cflash:]filename.cfg|none
```

Parameter

config Specifies the name of the configuration file to act as the active configuration file for the switch. The name can be from 1 to 16 alphanumeric characters, not including the extension “.cfg”. If the filename contains spaces, enclose it in double quotes.

Description

This command specifies the active configuration file on a switch. The switch uses the active configuration file to save its parameter settings when the SAVE CONFIGURATION command is issued, and to configure its settings when reset or power cycled.

Before using this command, note the following:

- To view the name of the currently active configuration file, see “SHOW CONFIG” on page 270.
- The configuration file must already exist. To view the files, see “SHOW FILE” on page 272. Configuration files have a “.cfg” extension. To create an entirely new configuration file, refer to “CREATE CONFIG” on page 259.
- Changing the active boot configuration file does not change the current operating configuration of the switch. You must reset or power cycle the switch after specifying the new active boot configuration file if you want the switch to use the settings in the file.
- If you specify a new active configuration file and enter the SAVE CONFIGURATION command without resetting the switch, the current settings of the switch overwrite the settings in the file.
- The NONE option does the following:
    - It removes the currently active configuration file without assigning a new one.
    - The switch continues to operate with its existing configuration settings.
    - You may make further parameter changes, but you cannot save them.
    - If you reset the switch, it uses the BOOT.CFG file to configure its settings.
    - To be able to save configuration changes again, you must

assign a new active boot configuration file.

- For those systems that support a flash memory card, you can specify a configuration file on a flash card as the active boot configuration file for a switch. However, the configuration file is not copied to the switch’s file system, but is instead used and updated directly from the card. If you remove the card and reset the switch, the management software uses its default settings.
- If the file is on a flash memory card, you must change to the directory where the file is stored before performing this command. The command does not accept a directory path. To change directories on a flash card, see “SET CFLASH DIR” on page 265. The default location is the root of the flash card.

Examples

This command designates the switch22.cfg file as the new active boot configuration file for the switch:

```
set config=switch22.cfg
```

If you want the switch to use the settings in the file, you reset or power cycle the unit. If, instead, you want to overwrite the settings in the file with the switch’s current settings, you enter the SAVE CONFIGURATION command.

This command uses the NONE option to remove the current active boot configuration file without specifying a new one. The switch does not allow you to save any further changes to the switch’s configuration, though you can continue to make changes. If you reset the unit, it uses the BOOT.CFG file to configure its settings:

```
set config=none
```

This command specifies the file “sw sales.cfg” on a flash memory card as the switch’s active boot configuration file:

```
set config=cflash:”sw sales.cfg”
```

AlliedWare Plus Command

Syntax

```
boot config-file [cflash:]filename.cfg|none
```

Modes

Privileged Exec mode

Description

This AlliedWare Plus command differs from the standard command as follows:

- If you specify a new active configuration file for the switch, the command displays a confirmation prompt, asking if you want to overwrite the existing file. If you respond with yes, the existing file is overwritten with the switch’s current settings. If you respond with no, the file is not overwritten. In most cases, you will probably respond with no. As explained in the standard command, after designating a new boot configuration file, you must reset the switch if you want to configure the unit with the settings in the file.
- If you specify a new active boot configuration file and the file does not exist, the command creates it. In contrast, the standard command displays an error message.
- The filename must not have spaces.

Example

This command designates the file named SW12A.CFG as the switch’s active configuration file:

```
awplus# boot config-file sw12a.cfg
```

This command uses the NONE option to remove the current active boot configuration file without specifying a new one. The switch does not allow you to save any further changes to the switch’s configuration, though you can continue to make changes. If you reset the unit, it uses the BOOT.CFG file to configure its settings:

```
awplus# boot config-file none
```

This command specifies a configuration file named PRODUCTION.CFG on a flash memory card as the switch’s active boot configuration file:

```
awplus# boot config-file cflash:production.cfg
```

SHOW CFLASH

Syntax

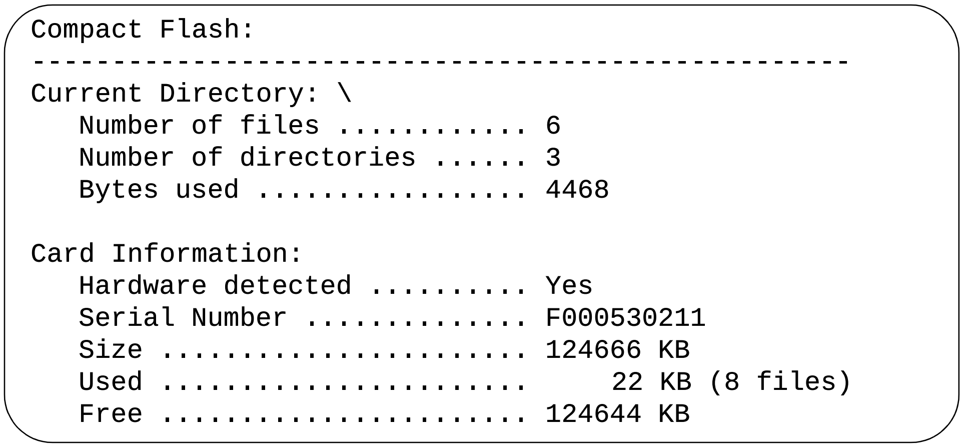
```
show cflash
```

Parameter

None

Description

This command displays information about the compact flash card including the current directory, the number of files, how much space is used, and amount of space available. An example is shown in Figure 48.



```
Compact Flash:
---------------------------------------------------
Current Directory: \
   Number of files ............ 6
   Number of directories ...... 3
   Bytes used ................. 4468

Card Information:
   Hardware detected .......... Yes
   Serial Number .............. F000530211
   Size ....................... 124666 KB
   Used .......................     22 KB (8 files)
   Free ....................... 124644 KB
```

Figure 48. SHOW CFLASH Command

Example

```
show cflash
```

SHOW CONFIG

AlliedWare Plus
Command
Available

Syntax

```
show config [dynamic]
```

Parameter

dynamic Displays the settings for all the switch and port parameters in command line format.

Description

This command, when used without the DYNAMIC parameter, displays two pieces of information. The first is the “Boot configuration file.” This is the configuration file the switch uses the next time it is reset or power cycled. This is also the configuration file the switch uses to save your configuration changes when you use the SAVE CONFIGURATION command. To change the boot configuration file, refer to “SET CONFIG” on page 266.

The second piece of information is the “Current Configuration.” This is the boot configuration file the switch used the last time it was reset or power cycled.

An example of the information displayed by the command is shownn in Figure 49.

```
Boot configuration file .............. "SalesSw4a.cfg" (Exists)
Current configuration ................ "SalesSw4a.cfg"
```

Figure 49. SHOW CONFIG Command

The DYNAMIC parameter displays all the switch settings in command line format for those switch parameters that have been changed from their default settings. For an example of the information displayed by the command, refer to Figure 29 on page 92.

Example

The following command displays the names of the active and current configuration files:

```
show config
```

AlliedWare Plus Command

Syntax

```
show boot
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command without the DYNAMIC parameter.

Example

```
awplus> show boot
```

SHOW FILE

AlliedWare Plus
Command
Available

Syntax

```
show file[=[cflash:]filename.ext]
```

Parameter

file	Specifies the name of the file to be displayed. Use double quotes to enclose the name if it contains spaces. Otherwise, the quotes are optional. To view a file on a flash memory card, precede the name with “cflash”. If you do not specify a file name, the command lists all the files in the flash memory as well as on a compact flash card, if one is installed in the switch.

Description

This command lists the files in the switch’s file system. You can use the wildcard “*” to replace any part of the filename to allow a more selective display.

You can also use this command to view the contents of a configuration file.

Examples

The following command displays all the files in the switch’s file system and the current directory of the flash memory card:

```
show file
```

The following command displays all the configuration files on the switch:

```
show file=*.cfg
```

The following command displays the contents of the configuration file sw12.cfg in the switch’s file system:

```
show file=sw12.cfg
```

The following command displays the contents of the configuration file boot.cfg on a compact flash card:

```
show file=cflash:boot.cfg
```

AlliedWare Plus Command

Syntax

```
ls [[cflash:]filename.ext]
```

```
dir [[cflash:]filename.ext]
```

Mode

User Exec mode and Privileged Exec mode

Description

Both of these AlliedWare Plus commands are identical to the standard command.

Example

This example lists all the files in the file system:

```
awplus> ls
```

This example lists just the configuration files:

```
awplus> ls *.cfg
```

This example displays the contents of the “boot.cfg” file:

```
awplus> ls boot.cfg
```

This example lists all the files in the file system:

```
awplus> dir
```

This example lists just the configuration files:

```
awplus> dir *.cfg
```

This example displays the contents of the “sw12.cfg” file:

```
awplus> dir sw12.cfg
```

SHOW FLASH

AlliedWare Plus Command Available

Syntax

```
show flash
```

Parameter

None

Description

This command displays information about the file system in the switch. The information includes the number of files stored in the file system, how much space is used, and the amount of space available. An example is shown in Figure 50.

```
Flash:
----------------------------------------------------
  Files ............. 12288 bytes (5 files)
  Free  ............. 8211456 bytes
  Total .............. 8223744 bytes
----------------------------------------------------
```

Figure 50. SHOW FLASH Command

Example

```
show flash
```

AlliedWare Plus Command

Syntax

```
show file systems
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the same information as the standard command and lists the files in the file system.

Example

```
awplus# show file systems
```

Chapter 16

File Download and Upload Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

LOAD METHOD=LOCAL

Syntax

```
load method=local destfile=appblock
srcfile|file=[cflash:]filename
```

Parameters

method	Specifies a local download.
destfile	Specifies the application block (APPBLOCK) of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S63 image file.
srcfile *or* file	Specifies the filename of the AT-S63 image file in the file system to be downloaded into the application block. If the image file is stored on a compact flash card, precede the filename with "cflash:". If the filename contains a space, enclose it in double quotes. These parameters are equivalent.

Description

This command downloads an AT-S63 image file from the switch's file system into the application block, which is the section of flash memory reserved for the active AT-S63 running image. This function makes the AT-S63 file the new active image file on the switch. This command assumes that at some earlier point you downloaded a new version of the AT-S63 image file into the file system of a switch and now want to copy it into application block so that it becomes the switch's active image file.

This command can also be used to download an AT-S63 image file from a compact flash card into the application block.

When performing a local download, note the following:

- The AT-S63 management image file must already be stored in the switch's file system or on a compact flash card.
- The command must include the DESTFILE parameter with the APPBLOCK option.
- Use the SRCFILE or FILE parameter to specify the name of the AT-S63 image file in the switch's file system or on the compact flash card.
- The current configuration of a switch is retained when a new AT-S63 software image is copied to the application block.

❒ After downloading an image file into the application block, you can delete the image file from the file system or compact flash card to free up space for other files.

⚠ **Caution**
The switch, after downloading the AT-S63 image file into its application block, automatically resets to initialize the new management software. The entire process takes about a minute. The switch does not forward network traffic during the reset process. Some network traffic may be lost.

Examples

This command downloads an AT-S63 image file stored in the switch’s file system into the application block, the area of flash memory reserved for the active running image. This makes the file the active image file on the switch. The name of the image file in the file system in this example is “ats63v2.img”:

```
load method=local destfile=appblock srcfile=”ats63v2.img”
```

A confirmation prompt is displayed. Type **Y** for yes to transfer the file to the application block or **N** for no to cancel the procedure.

This command downloads an AT-S63 image file from a compact flash card to the switch’s application block. The name of the image file on the compact flash card is “ats63v2.img”:

```
load method=local destfile=appblock
srcfile=cflash:”ats63v2.img”
```

LOAD METHOD=TFTP

AlliedWare Plus
Command
Available

Syntax 1: Downloading Files to the File System

```
load method=tftp destfile=[cflash:]filename
server=ipaddress srcfile|file=filename
```

Syntax 2: Downloading New AT-S63 Management Software to a Stand-alone Switch

```
load method=tftp destfile=appblock server=ipaddress
srcfile|file=filename
```

Syntax 3: Downloading New AT-S63 Management Software to an AT-9400 Stack

```
load method=tftp destfile=appblock server=ipaddress
srcfile|file=filename module=value|all
```

Parameters

method — Specifies a TFTP download.

destfile — Specifies the destination filename for the file. If you are downloading a configuration file or a SSL public key certificate, this is the name given to the file when it is stored in the switch’s file system. The name can be from 1 to 15 alphanumeric characters, not including the three-letter extension. If the name includes spaces, enclose it in double quotes. The name must be unique from the files already stored in the file system. The command will not overwrite a preexisting file.

To download a file onto a flash memory card in the switch rather than the file system, precede the name with “cflash:”.

If you are downloading new AT-S63 Management Software, specify APPBLOCK as the destination. This specifies the application block, which is an area of the switch’s flash memory reserved for the active AT-S63 image file.

server — Specifies the IP address of the TFTP server on the network.

srcfile ***or*** file — Specifies the filename of the file on the TFTP server to download onto the switch. If the filename contains a space, enclose the name in double quotes. These parameters are equivalent.

module Specifies the switches in the AT-9400 Stack to receive the new AT-S63 Management Software. The range is 1 to 8. You can specify more than one switch (e.g., 1,2). To update all the switches, use ALL.

General Description

These commands are used to download files and new versions of the AT-S63 Management Software to stand-alone switches and stacks, using TFTP.

Note
In earlier versions of the AT-S63 Management Software this command also performed switch to switch file transfers for copying files from a master switch to other switches in an enhanced stack. That function is now part of "UPLOAD METHOD=REMOTESWITCH" on page 292

Syntax 1 Description

This command is used to download configuration files and SSL public key certificates to the file system on the switch. This command can be used on both stand-alone switches and stacks. If you are using this command on a stack, you can download files only to the file system of the master switch.

When specifying the new name of a downloaded file, be sure to give it the correct three-letter extension that corresponds to its file type. The extensions are shown in Table 5.

Table 5. File Name Extensions - Downloading Files

Extension	File Type
.cfg	Configuration file
.cer	SSL public key certificate

To store a file in a flash memory card, precede the destination filename with "cflash:".

This command can also be used to download new AT-S63 Management Software to the file system in a switch, though it is unlikely you will use this function. New management software has to be stored in the application block of flash memory, not the file system, to act as the switch's new management software. If you do download new management software into the file system and later want to copy it to the application block, use "LOAD METHOD=LOCAL" on page 276.

Syntax 2 Description

This command is used to download new AT-S63 Management Software to stand-alone switches. The destination is APPBLOCK, the area in flash memory reserved for this file and called the application block.

⚠ **Caution**
This command will disrupt network operations. The switch will reset after writing the new AT-S63 Management Software to the application block portion of flash memory. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

Syntax 3 Description

This command is used to download new AT-S63 Management Software to AT-9400 Stacks. As in Syntax 2, the destination should be APPBLOCK.

You use the MODULE parameter to specify the switches in the stack to be updated. In most cases you should enter ALL. But you can update individual switches by entering their stack ID numbers, instead.

Note
The MODULE parameter only works on switches with Version 4.0.0 or later of the AT-S63 Management Software. To update a stack that has an earlier version of the management software, remove the switches from the stack by disconnecting the stacking cables and update them as stand-alone units. For more information, refer to the software release notes.

⚠ **Caution**
This command will disrupt network operations. The switch will reset after writing the new AT-S63 Management Software to the application block portion of flash memory. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

Guidelines

Before downloading a file onto a switch using TFTP, note the following:

❒ A TFTP download is supported from a local, Telnet or SSH management session.

- There must be a node on your network with the TFTP server software and the file to be downloaded must be stored on the server.
- You should start the TFTP server software before performing the download command.
- For AT-9400 Switches running AT-S63 version 2.0.0 or later, the switch must have a routing interface on the local subnet from where it reaches the TFTP server. The switch uses the interface’s IP address as its source address during the file transfer with the server. This rule applies equally to master and slave switches in an enhanced stack. For AT-9400 Switches without a routing interface, you can perform an Xmodem download from a local management session or, alternatively, a switch to switch upload using “UPLOAD METHOD=REMOTESWITCH” on page 292.
- For AT-9400 Switches running AT-S63 version 1.3.0 or earlier, the switch must be able to access the TFTP server through its management VLAN.
- If you are upgrading the AT-9400 Switch from AT-S63 version 1.3.0 or earlier and the switch has an IP address, the upgrade process automatically creates a routing interface on the switch to preserve the device’s IP configuration. If the switch has a static address, the interface is assigned the same address. If the unit obtains its IP configuration from a DHCP or BOOTP server, the interface is created with its DHCP or BOOTP client activated. The interface is given the interface number 0 and assigned to the preexisting management VLAN. Furthermore, the interface is designated as the local interface on the switch.

  For example, if the switch has the static IP address 149.44.44.44 and the management VLAN has a VID of 12, the upgrade process automatically creates a routing interface with the same IP address and names it VLAN12-0. It assigns the interface to the VLAN with the VID of 12 and designates it as the switch’s local interface.
- If you download a configuration file, the switch receiving the file does not automatically designate it as its active boot configuration file. To designate a configuration file as the active boot file after you have downloaded it onto the switch, refer to “SET CONFIG” on page 266.
- The AT-S63 Management Software can be downloaded only onto an AT-9400 Switch.
- The current configuration of a switch is retained when a new AT-S63 software image is installed.
- The AT-S63 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- If you download a new AT-S63 image file and enter a filename for the DESTFILE parameter instead of APPBLOCK, the file is stored in the switch’s file system. To copy the image file from the file system to the

application block so that its used by the switch as its active image file, refer to “UPLOAD METHOD=LOCAL” on page 290.

Note
Downloading an AT-S63 image file into a switch’s file system rather than into the application block should be perform with care. The file will take up 2 megabytes of space in the file system.

❒ If you download a file onto a flash memory card in the switch and later want to copy the file from the card to a switch’s file system, refer to “COPY” on page 256.

Syntax 1 Examples

This command downloads a new configuration file into the switch’s file system using TFTP. The file is stored as “sw 111.cfg” on the TFTP server and is given the name “sw56a.cfg” when it is stored in the switch’s file system. The TFTP server has the IP address 149.55.55.55:

```
load method=tftp destfile=sw56a.cfg server=149.55.55.55
srcfile=”sw 111.cfg”
```

This command downloads an SSL certificate to the switch’s file system. The file, which has the name “sw12_ssl.cer” on the TFTP server, retains the same name when it is stored in the file system:

```
load method=tftp destfile=sw12_ssl.cer server=149.44.44.44
srcfile=sw12_ssl.cer
```

This command downloads a configuration file called “sw12.cfg onto a flash memory card in the switch. The filename remains the same. The TFTP server has the IP address 149.142.44.44:

```
load method=tftp destfile=cflash:sw12.cfg
server=149.142.44.44 srcfile=sw12.cfg
```

This command downloads a new version of the AT-S63 image file from a TFTP server to the switch’s file system, changing the name from “ats63v1_2_0.img” to “ats63.img”:

```
load method=tftp destfile=ats63.img server=149.11.11.11
srcfile=ats63v1_2_0.img
```

Since the file is downloaded to the switch’s file system and not to the application block, it is not used as the switch’s active image file. If at some point in the future you want to make it the active image file, refer to “UPLOAD METHOD=LOCAL” on page 290.

This command downloads an AT-S63 image file from a TFTP server to a flash memory card in the switch:

```
load method=tftp destfile=cflash:ats63.img
server=149.11.11.11 srcfile=ats63.img
```

Syntax 2 Example

This command downloads new AT-S63 Management Software to the application block of a stand-alone switch, making the software the active image file on the unit. The IP address of the TFTP server is 149.11.11.11 and the name of the image file on the server is “ats63v4.img”:

```
load method=tftp destfile=appblock server=149.11.11.11
srcfile=ats63v4.img
```

Syntax 3 Examples

This command updates the AT-S63 Management Software on all the switches in an AT-9400 Stack, The IP address of the TFTP server is 122.124.54.78 and the name of the file is “ats63_new.img”:

```
load method=tftp destfile=appblock server=122.124.54.78
srcfile=ats63_new.img module=all
```

This command updates the AT-S63 Management Software on just the member switch assigned the stack ID 3. The IP address of the TFTP server is 155.174.12.52 and the name of the file is “ats63.img”:

```
load method=tftp destfile=appblock server=155.174.12.52
srcfile=ats63.img module=3
```

AlliedWare Plus Command

Syntax

```
download tftp ipaddress filename.img
```

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is used to download new versions of the AT-S63 Management Software from a TFTP server into the application block in stand-alone switches. The IPADDRESS parameter is the IP address of the TFTP server and the FILENAME.IMG parameter is the name of the file of the new management software on the server.

You cannot used this command to download files into a switch’s file system or compact flash card. You also cannot use this command to download new AT-S63 Management Software to AT-9400 Stacks.

Example

This example downloads the file “ats63_app.img” into the application block of a switch. The TFTP server has the IP address 149.22.121.45:

```
awplus> enable
awplus# download tftp 149.22.121.45 ats63_app.img
```

LOAD METHOD=XMODEM

AlliedWare Plus
Command
Available

Syntax 1: Downloading Files to the File System

```
load method=xmodem destfile=[cflash:]filename
```

Syntax 2: Downloading New AT-S63 Management Software to a Stand-alone Switch

```
load method=xmodem destfile=appblock
```

Syntax 3: Downloading New AT-S63 Management Software to an AT-9400 Stack

```
load method=xmodem destfile=appblock module=value|all
```

Parameters

method — Specifies a XMODEM download.

destfile — Specifies the destination filename for the file. If you are downloading a configuration file or a SSL public key certificate, this is the name given to the file when it is stored in the switch's file system. The name can be from 1 to 15 alphanumeric characters, not including the three-letter extension. If the name includes spaces, enclose it in double quotes. The name must be unique from the files already stored in the file system. The command will not overwrite a preexisting file.

To download a file onto a flash memory card in the switch rather than the file system, precede the name with "cflash:".

If you are downloading new AT-S63 Management Software, specify APPBLOCK as the destination. This specifies the application block, which is the area of flash memory reserved for the active AT-S63 image file.

module — Specifies the switches in the AT-9400 Stack to receive the new AT-S63 Management Software. The range is 1 to 8. You can specify more than one switch (e.g., 1,2). To update all the switches, use ALL.

General Description

These commands are used to download files and new versions of the AT-S63 Management Software to stand-alone switches and stacks, using XMODEM.

Note

In earlier versions of the AT-S63 Management Software this command also performed switch to switch file transfers for copying files from a master switch to other switches in an enhanced stack. That function is now part of “UPLOAD METHOD=REMOTESWITCH” on page 292

Syntax 1 Description

This command is used to download configuration files and SSL public key certificates to the file system on the switch. This command can be used on both stand-alone switches and stacks. If you are using this command on a stack, you can only download files to the file system of the master switch.

When specifying the new name of a downloaded file, be sure to give it the correct three-letter extension that corresponds to its file type. The extensions are shown in Table 5 on page 279.

To store a file in a flash memory card, precede the destination filename with “cflash:”.

Syntax 2 Description

This command is used to download new AT-S63 Management Software to stand-alone switches. The destination is APPBLOCK, the area in flash memory reserved for this file and called the application block.

If you specify a filename instead of APPBLOCK, the file is stored in the switch’s file system. Copying it from the file system to the application block is accomplished with “LOAD METHOD=LOCAL” on page 276.

⚠ **Caution**

This command will disrupt network operations. The switch will reset after writing the new AT-S63 Management Software to the application block portion of flash memory. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

Syntax 3 Description

This command is used to download new AT-S63 Management Software to AT-9400 Stacks. As in Syntax 2, the destination should be APPBLOCK.

You use MODULE parameter to specify the switches in the stack to be updated. In most cases you should enter ALL. But you can update individual switches by entering their stack ID numbers, instead.

Note

The MODULE parameter only works on switches with Version 4.0.0 or later of the AT-S63 Management Software. To update a stack that has an earlier version of the management software, remove the switches from the stack by disconnecting the stacking cables and update them as stand-alone units. For more information, refer to the software release notes.

⚠ **Caution**

This command will disrupt network operations. The switch will reset after writing the new AT-S63 Management Software to the application block portion of flash memory. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

Guidelines

Before downloading a file onto a switch using XMODEM, note the following:

- You must use a local management session to download a file using Xmodem.
- You can only use Xmodem to download a file onto the switch where you started the local management session. You cannot use it to download a file onto a switch accessed through enhanced stacking.
- You must store the file to be downloaded on the computer or terminal connected to the RS232 Terminal Port on the switch.
- The transfer protocol can be Xmodem or 1K Xmodem.
- The switch does not automatically designate a newly downloaded configuration file as its active boot configuration file. To designate the active boot file, refer to “SET CONFIG” on page 266.
- The AT-S63 software image is only supported on AT-9400 Switches.
- The current configuration of a switch is retained when a new AT-S63 software image is installed.
- The AT-S63 image file also contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- If you download a new AT-S63 image file and enter a filename for the DESTFILE parameter instead of APPBLOCK, the file is stored in the switch’s file system. To copy an image file from the file system to the switch’s application block, refer to “LOAD METHOD=LOCAL” on page 276.

- ❒ If you download a file onto a flash memory card in the switch and later want to copy the file from the card to a switch's file system, refer to "COPY" on page 256.
- ❒ If you are upgrading the AT-9400 Switch from AT-S63 version 1.3.0 or earlier and the switch has an IP address, the upgrade process automatically creates a routing interface on the switch to preserve the device's IP configuration. If the switch has a static address, the interface is assigned the same address. If the unit obtained its IP configuration from a DHCP or BOOTP server, the interface is created with its DHCP or BOOTP client activated. The interface is given the interface number 0 and assigned to the preexisting management VLAN. Furthermore, the interface is designated as the local interface on the switch.

  For example, if the switch has the static IP address 149.44.44.44 and the management VLAN has a VID of 12, the upgrade process automatically creates a routing interface with the same IP address and names it VLAN12-0. It assigns the interface to the VLAN with the VID of 12 and designates it as the switch's local interface.

Syntax 1 Examples

This command downloads a new configuration file and gives it the name "switch2a.cfg" in the switch's file system:

```
load method=xmodem destfile=switch2a.cfg
```

The source file is not specified when downloading a file with Xmodem. Rather, after you enter the command, the management software displays a confirmation prompt followed by another prompt that instructs you to begin the file transfer. To start the transfer, you specify the file with your terminal emulation program:

This command uses Xmodem to download an SSL certificate into the switch's file system and assigns it the name sw12 ssl.cer:

```
load method=xmodem destfile=”sw12 ssl.cer”
```

This command downloads a configuration file onto a flash memory card in the switch. The configuration file is given the name "product_sw.cfg" on the card:

```
load method=xmodem destfile=cflash:product_sw.cfg
```

This command downloads a new version of the AT-S63 image file to the switch's file system instead of the application block. It does this by replacing the APPBLOCK option with a filename, in this case "ats63v1_2_0.img". The image file is stored in the switch's file system with this name:

```
load method=xmodem destfile=ats63v1_2_0.img
```

Since the file is stored in the switch’s file system and not the application block, the switch does not use it as its active image file. If, at some point in the future, you want to make it the active image file, use “LOAD METHOD=LOCAL” on page 276.

Syntax 2 Example

This command downloads new AT-S63 Management Software into the application block of a stand-alone switch, making it the active image file on the switch:

```
load method=xmodem destfile=appblock
```

Syntax 3 Examples

This command updates the AT-S63 Management Software on all the switches in an AT-9400 Stack:

```
load method=xmodem destfile=appblock module=all
```

This command updates the AT-S63 Management Software on just the member switch assigned the stack ID 2:

```
load method=xmodem destfile=appblock module=2
```

AlliedWare Plus Command

Syntax

```
download serial
```

Mode

Privileged Exec mode

Description

This AlliedWare Plus command is used to download new versions of the AT-S63 Management Software into the application block on stand-alone switches. The file is downloaded using Xmodem through the terminal port on the unit. After entering the command, use your terminal emulation program to select the file to download onto the switch.

This command cannot be used to download files, such as configuration files, into the file system of the switch. For this, use “LOAD METHOD=XMODEM” on page 285.

Example

```
awplus> enable
awplus# download serial
```

UPLOAD METHOD=LOCAL

Syntax

```
upload method=local destfile=[cflash:]filename
srcfile|file=appblock
```

Parameters

method	Specifies a local upload.
destfile	Specifies a filename for the AT-S63 image file. If the name contains spaces, enclose the name in quotes. To upload the active image file to a flash memory card in the switch, precede the name with “cflash:”.
srcfile *or* file	Specifies the application block (APPBLOCK), where the active AT-S63 image file is stored.

Description

This command copies the switch’s active AT-S63 image file from the application block, where the active AT-S63 image is stored, into the switch’s file system or to a flash memory card.

> **Note**
> It is unlikely you will ever need to perform this type of upload.

The DESTFILE parameter specifies a name for the file. This is the name given to the AT-S63 image file when it is stored in the file system or on a compact flash memory card. The name should include the suffix “.img”.

The equivalent SRCFILE and FILE parameters specify APPBLOCK, for application block.

Examples

The following command uploads the active AT-S63 image from the switch’s application block to the file system and assigns it the name “sw12 s63 image.img”:

```
upload method=local destfile=”sw12 s63 image.img”
srcfile=appblock
```

This command uploads the active AT-S63 image from the switch’s application block to a flash memory card in the switch and assigns the name “s63.img” to the file:

```
upload method=local destfile=cflash:s63.img”
srcfile=appblock
```

UPLOAD METHOD=REMOTESWITCH

Syntax

```
upload method=remoteswitch
srcfile|file=filename|appblock|switchcfg
switchlist=switches [verbose=yes|no|on|off|true|false]
```

Parameters

method
Specifies a switch to switch upload.

srcfile *or* file
Specifies the file to be uploaded from the master switch. Options are:

filename	Uploads a configuration file from the master switch's file system.
appblock	Uploads the master switch's AT-S63 image file.
switchcfg	Uploads the master switch's active boot configuration file.

switchlist
Specifies the switches in an enhanced stack to receive the uploaded file. To view the switches, refer to "SHOW REMOTELIST" on page 114. You can specify more than one switch at a time (for example, 1,3,4).

verbose
Specifies whether to display details of the upload operation. The options are:

yes, on, true	Display the upload details. The options are equivalent.
no, off, false	Do not display the upload details. The options are equivalent.

Description

This command uploads the AT-S63 file image or a boot configuration file from a master switch to other switches in an enhanced stack. This is refer to as a switch to switch upload. You can use this command to simplify the task of updating the AT-S63 image file in the switches of an enhanced stack. By updating the image file on the master switch first, you can instruct the master switch with this command to update the other switches in the stack, automatically.

You can also use this command to distribute a configuration file on the master switch to other switches when switches are to share a similar configuration.

The equivalent SRCFILE and FILE parameters specify the name of the file to be uploaded from the switch. You have three options:

- *filename* - Uploads a configuration file from the master switch's file system. The filename must include the ".cfg" suffix.
- APPBLOCK - Uploads the master switch's active AT-S63 image file.
- SWITCHCFG - Uploads the master switch's active boot configuration file. You can use this option in place of the *filename* option when uploading the active boot configuration file on the master switch.

The SWITCHLIST parameter specifies the switches in the enhanced stack to receive the uploaded file. You display the switch numbers using "SHOW REMOTELIST" on page 114.

The optional VERBOSE parameter displays information about the progress of the upload process.

When performing a switch to switch upload, note the following:

- The command can be performed from a local, Telnet, or SSH management session of a master switch.
- You must perform the SHOW REMOTELIST command prior to this command to display the switch numbers and allow the management software to determine the number of switches in the enhanced stack. For instructions, refer to "SHOW REMOTELIST" on page 114.
- This command can upload the master switch's active AT-S63 image file or a configuration file to another switch. This command cannot upload any other type of file, such as an encryption key or SSL certificate.
- An uploaded configuration file retains its original name.
- The manager and operator passwords are included in the upload of a configuration file.
- When uploading the master switch's active AT-S63 image file, the file is copied directly to the application block on the other switch. This automatically designates it as the switch's active image file. The switch receiving the image file resets and initializes the new image file. Some network traffic may be lost during the reset process.
- If you are upgrading the AT-9400 Switch from AT-S63 version 1.3.0 or earlier and the switch has an IP address, the upgrade process automatically creates a routing interface on the switch to preserve the device's IP configuration. If the switch has a static address, the interface is assigned the same address. If the unit obtained its IP configuration from a DHCP or BOOTP server, the interface is created

with its DHCP or BOOTP client activated. The interface is given the interface number 0 and assigned to the preexisting management VLAN. Furthermore, the interface is designated as the local interface on the switch.

For example, if the switch has the static IP address 149.44.44.44 and the management VLAN has a VID of 12, the upgrade process automatically creates a routing interface with the same IP address and names it VLAN12-0. It assigns the interface to the VLAN with the VID of 12 and designates it as the switch's local interface.

❒ After receiving a configuration file, a switch automatically marks it as its active boot configuration file and resets. Some network traffic may be lost while the switch initializes its operating software. After the reset is complete, the switch operates with the parameter settings contained in the uploaded configuration file.

❒ If the file system of a switch receiving a configuration file already contains a file with the same name, the existing file is overwritten.

❒ Uploading the same configuration file onto more than one switch can cause an IP address conflict among the devices if the file contains commands for creating routing interfaces. To resolve the issue, after uploading the file you must modify the interfaces on the switches by changing the IP addresses.

❒ A configuration file should only be uploaded onto a switch of the same model as the unit where the file was created (for example, AT-9408LC/SP to AT-9408LC/SP). Allied Telesis does not recommend uploading a configuration file onto a switch of a different model (for example, AT-9408LC/SP to AT-9424T/SP). Undesirable switch behavior may result.

❒ This command does not support uploading files to or from a compact flash memory card.

Examples

The following command uploads the AT-S63 image file on a master switch to switch 2 in an enhanced stack. (Switch numbers are displayed with "SHOW REMOTELIST" on page 114.)

```
upload method=remoteswitch srcfile=appblock switchlist=2
```

The active AT-S63 image file on the master switch is indicated with the APPBLOCK option of the SRCFILE parameter.

Caution
After receiving the AT-S63 image file, the switch resets and initializes its software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

You can upload the AT-S63 image file from the master switch to more than one switch at a time. The following command uploads the image file to switches 4, 8, and 15:

```
upload method=remoteswitch srcfile=appblock
switchlist=4,8,15
```

The following command uploads the switch active boot configuration file from the master switch to switch 11:

```
upload method=remoteswitch srcfile=switchcfg switchlist=11
```

Caution
After receiving the configuration file the switch resets and initializes the software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

The following command uploads the configuration file “sales_switches.cfg” from a master switch to switch 4:

```
upload method=remoteswitch srcfile=sales_switches.cfg
switchlist=4
```

Caution
After receiving the configuration file the switch resets and initializes the software. The entire process can take a minute or so to complete. Do not interrupt the process by resetting or power cycling the switch. Some network traffic may be lost during the process.

UPLOAD METHOD=TFTP

Syntax

```
upload method=tftp destfile=filename server=ipaddress
srcfile|file=switchcfg|[cflash:]filename|appblock
```

Parameters

method	Specifies a TFTP upload.	
destfile	Specifies a filename for the uploaded file. This is the name given the file when it is stored on the TFTP server. If the name contains spaces, enclose it in quotes.	
server	Specifies the IP address of the network node containing the TFTP server software.	
srcfile *or* file	Specifies the file to be uploaded. Options are:	
	switchcfg	Uploads the switch’s active boot configuration file.
	filename	Uploads a file from the switch’s file system. If the file is stored on a compact flash card, precede the name with “cflash:”.
	appblock	Uploads the switch’s active AT-S63 image file.

Description

A TFTP upload uses the TFTP client software on the switch to upload files from the file system on the system to a TFTP server on the network. You can use the command to upload a switch’s active boot configuration file or any other file from the file system, such as an SSL certificate enrollment request or a public encryption key. This command can also upload a file from a compact flash memory card in the switch to a TFTP server. You can also use the command to upload the switch’s active AT-S63 software image from the application block to a TFTP server, though it is unlikely you would ever have need for that function.

When performing a TFTP upload, note the following:

- A TFTP upload is supported from a local, Telnet, or SSH management session.
- There must be a node on your network that contains the TFTP server software. The uploaded file will be stored on the server.

- Start the TFTP server software before you perform the command.
- The AT-9400 Switch must have a routing interface on the local subnet from where it is reaching the TFTP server. The switch uses the interface's IP address as its source address during the file transfer with the server. This rule applies equally to master and slave switches in an enhanced stack. The server can be located on any interface on the switch, not just the local interface. If the AT-9400 Switch does not have a routing interface, you can perform an Xmodem upload from a local management session or, alternatively, a switch to switch upload using "UPLOAD METHOD=REMOTESWITCH" on page 292.

The DESTFILE parameter specifies a name for the file. This is a name for the file when it is stored on the TFTP server. The uploaded file should be given the same three-letter extension as the original file. The extensions are listed in Table 6.

Table 6. File Name Extensions - Uploaded Files

Extension	File Type
.cfg	Switch configuration file
.csr	CA certificate enrollment request
.log	Event log
.key	Public encryption key
.img	AT-S63 Management Software image

The SERVER parameter specifies the IP address of the network node with the TFTP server software where the uploaded file will be stored.

The equivalent SRCFILE and FILE parameters specify the name of the file to be uploaded from the switch. You have three options:

- SWITCHCFG - Uploads the switch's active boot configuration file to the TFTP server.
- *filename* - Uploads a file from the switch's file system to the TFTP server. This differs from the SWITCHCFG parameter in that the latter uploads just the active boot configuration file, while this parameter can upload any file in the file system. If the file to be uploaded is stored on a compact flash memory card in the switch, precede the name with "cflash:".
- APPBLOCK - Uploads the switch's active AT-S63 image file to the TFTP server.

Note
It is unlikely you will ever need to upload the active AT-S63 image file from a switch to a TFTP server. If you need the image file to transfer to another switch, you can simplify the process with a switch to switch upload using “UPLOAD METHOD=REMOTESWITCH” on page 292. Alternatively, you can obtain the latest version of the image file from the Allied Telesis web site.

Examples

The following command uses TFTP to upload a configuration file called “sw22 boot.cfg” from the switch’s file system to a TFTP server with an IP address of 149.88.88.88. The command stores the file on the server with the same name that it has on the switch:

```
upload method=tftp destfile="sw22 boot.cfg"
server=149.88.88.88 srcfile="sw22 boot.cfg"
```

The following command uses TFTP to upload the switch’s active configuration file from the file system to a TFTP server with the IP address 149.11.11.11. The active boot file is signified with the SWITCHCFG option rather than by its filename. This option is useful in situations where you do not know the name of the active boot configuration file. The file is stored as “master112.cfg” on the TFTP server:

```
upload method=tftp destfile=master112.cfg
server=149.11.11.11 srcfile=switchcfg
```

The following command uploads a SSL certificate enrollment request form titled “sw12_ssl_enroll.csr” from the file system to the TFTP server. It changes the name of the file to “slave5b enroll.csr”:

```
upload method=tftp destfile="slave5b enroll.csr"
server=149.11.11.11 srcfile=sw12_ssl_enroll.csr
```

The following command uploads a configuration file called “sales2.cfg” from a compact flash memory card in the switch to a TFTP server with an IP address of 149.124.88.88. The command stores the file on the server with the same name that it has on the card:

```
upload method=tftp destfile=sales2.cfg server=149.124.88.88
srcfile=cflash:sales2.cfg
```

The following command uploads the switch’s active AT-S63 image file to a TFTP server with an IP addresses 149.55.55.55. The file is given the name “ats63 sw12.img”:

```
upload method=tftp destfile="ats63 sw12.img"
server=149.55.55.55 srcfile=appblock
```

UPLOAD METHOD=XMODEM

Syntax

```
upload method=xmodem
srcfile|file=switchcfg|[cflash:]filename|appblock
```

Parameters

method Specifies an Xmodem upload.

srcfile *or* file Specifies the file to be uploaded. Options are:

switchcfg	Uploads the switch’s active boot configuration file.
filename	Specifies the name of a file to upload from the switch’s file system or compact flash card. If the file is stored on a compact flash card, precede the name with “cflash:”.
appblock	Uploads the switch’s active AT-S63 image file.

Description

An XMODEM upload uses the Xmodem utility to upload a file from the switch’s file system to a terminal or computer with a terminal emulator program connected to the serial terminal port on the switch. You can use the command to upload a switch’s active boot configuration file or any other file from the file system, such as an SSL certificate enrollment request or a public encryption key. You can also use this command to upload a file on a compact flash memory card to your workstation. The command also allows you to upload the switch’s active AT-S63 software image from the application block to a your terminal or workstation, though it is unlikely you would ever have need for that function.

When performing an Xmodem upload, note the following:

- An Xmodem upload must be performed from a local management session.
- Xmodem can only upload a file from the switch where you started the local management session. Xmodem cannot upload a file from a switch accessed through enhanced stacking.

The equivalent SRCFILE and FILE parameters specify the name of the file to upload from the switch. You have three options:

❐ SWITCHCFG - Uploads the switch’s active boot configuration file.

❐ *filename* - Uploads a file from the switch’s file system or a compact flash memory card. This differs from the SWITCHCFG parameter in that the latter can upload just the active boot configuration file, while this parameter can upload any file on the switch. If the file is stored on a flash memory card in the switch, precede the filename with “cflash:”.

❐ APPBLOCK - Uploads the switch’s active AT-S63 image file.

> **Note**
> It is unlikely you will ever need to upload the active AT-S63 image file from a switch to your workstation. If you need the image file to transfer to another switch, you can simplify the process with a switch to switch upload using “UPLOAD METHOD=REMOTESWITCH” on page 292. Alternatively, you can obtain the latest version of the image file from the Allied Telesis web site.

Examples

The following command uses Xmodem to upload a configuration file called “sw22 boot.cfg” from the switch’s file system to your workstation:

```
upload method=xmodem srcfile="sw22 boot.cfg"
```

An Xmodem upload command does not include a destination filename. After entering the command, use your terminal emulator program to indicate where to store the file on your workstation and its filename.

The following command uploads the switch’s active configuration file from the file system to your workstation. The active boot file is signified with the SWITCHCFG option rather than by its filename. This option is useful in situations where you do not know the name of the active boot configuration file:

```
upload method=xmodem srcfile=switchcfg
```

The following command uploads a SSL certificate enrollment request named “sw12_ssl_enroll.csr” from the switch’s file system to the workstation:

```
upload method=xmodem srcfile=sw12_ssl_enroll.csr
```

The following command uses Xmodem to upload a configuration file called “pre10.cfg” from a flash memory card to the workstation where you are running the local management session:

```
upload method=xmodem srcfile=cflash:pre10.cfg
```

The following command uploads the switch’s active AT-S63 image file to the workstation:

```
upload method=xmodem srcfile=appblock
```

Chapter 17

Event Log and Syslog Client Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

ADD LOG OUTPUT

Syntax

```
add log output=output-id module=[all|module]
severity=[all|severity]
```

Parameters

output — Specifies the output definition ID number.

module — Specifies what AT-S63 events to filter. The available options are:

- all — Sends events for all modules. This is the default.
- module — Sends events for specific module(s). You can select more than one module at a time, for example, MAC,PACCESS. For a list of modules, see Table 9, “AT-S63 Modules” on page 327.

severity — Specifies the severity of events to be sent. The options are:

- all — Sends events of all severity levels.
- severity — Sends events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 329. The default is I, E, and W.

Description

This command configures an output definition.

> **Note**
> This version of the AT-S63 management software supports only syslog servers as output definitions.

There are two steps to creating a output definition from the command line interface. The first is to create the definition using “CREATE LOG OUTPUT” on page 306. With that command you assign the definition an ID number, the IP address of the syslog server, and other information.

The second step is to customize the definition by specifying which event messages generated by the switch are to be sent. This is accomplished with this command. You can customize the definition so that the switch sends all of its event messages or limit it to just a selection of events from particular modules in the AT-S63 management software. An alternative method to configuring a definition is with "SET LOG OUTPUT" on page 322.

Note
The default configuration for a new output definition is no event messages. The switch does not send any events until you customize the definition with this command or "SET LOG OUTPUT" on page 322.

The OUTPUT parameter specifies the ID number of the output definition you want to configure. The range is 2 to 20. The definition must already exist on the switch. To view the existing definitions and their ID numbers, refer to "SHOW LOG OUTPUT" on page 331.

The MODULE parameter specifies the modules whose events you want the switch to send. The AT-S63 management software consists of a number of modules. Each module is responsible for a different part of switch operation and generates its own events. The MODULE parameter's ALL option sends the events from all the modules. You can also specify individual modules, which are listed in Table 9 on page 327.

The SEVERITY parameter specifies the severity of the events to be sent. For example, you might configure the switch to send only error events of all the modules. Or, you might configure a definition so that the switch sends only warning events from a couple of the modules, such as the spanning tree protocol and the MAC address table. For a list of severity levels, refer to Table 10 on page 329.

Examples

The following command configures output definition 5 to send event messages from all modules and all severity levels:

```
add log output=3 module=all severity=all
```

The following command configures output definition 3 to send only messages related to enhanced stacking and the MAC address table with an error severity level:

```
add log output=3 module=estack,mac severity=e
```

CREATE LOG OUTPUT

AlliedWare Plus Command Available

Syntax

```
create log output=output-id destination=syslog
server=ipaddress
[facility=default|local1|local2|local3|local4|local5|local6
|local7] [syslogformat=extended|normal]
```

Parameters

output
: Specifies an ID number that identifies the output definition. The possible output IDs are:

0	Reserved for permanent (nonvolatile) storage. You cannot change or delete this ID.
1	Reserved for temporary (dynamic) storage. You cannot change or delete this ID.
2 - 20	Available to be used for other outputs.

destination
: Specifies the destination for the log messages. The only option currently supported is:

syslog	Forwards log messages in syslog format to a syslog server.

server
: Specifies the IP address of the syslog server.

facility
: Specifies a facility level to be added to the events.

default
: Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S63 management software and its modules are shown in Table 7 on page 308. This is the default setting.

local1 to local7
: Adds a set facility code of 17 (LOCAL1) to 23 (LOCAL7) to all event messages. For a list of the levels and their corresponding codes, refer to Table 8 on page 309.

syslogformat Specifies the format of the generated messages. The possible options are:

extended Messages include the date, time, and system name. This is the default.

normal Messages do not include the date, time, and system name.

Description

This command creates a new output definition. The switch uses the definition to send event messages to a device on your network. You can create up to nineteen output definitions.

Note
This version of the AT-S63 management software supports only syslog servers as output definitions.

Note
The switch must have a routing interface on the local subnet where the syslog server is a member. The switch uses the IP address of the interface as its source address when sending packets to the server. For instructions on how to add a routing interface to the switch, refer to “ADD IP INTERFACE” on page 708.

After creating a output definition with this command, you must customize it by defining which event messages you want the switch to send. You can customize a definition so that the switch sends all of its event messages or limit it to just a selection of events from particular modules in the AT-S63 management software. Customizing a definition is accomplished with “ADD LOG OUTPUT” on page 304 or “SET LOG OUTPUT” on page 322.

Note
The default configuration for a new output definition is no event messages. The switch does not send events until you customize the definition.

The OUTPUT parameter specifies the ID number for the new output definition. The range is 2 to 20. Every definition must have a unique ID number.

The SERVER parameter specifies the IP address of the syslog server.

The FACILITY parameter adds a numerical code to the entries as they are sent to the syslog server. You can use this code to group entries on the syslog server according to the management module or switch that produced them. This is of particular value when a syslog server is collecting events from several difference network devices. You can specify only one facility level for a syslog server definition.

There are two approaches to using this parameter. The first is to use the DEFAULT option. At this setting, the code is based on the functional groupings defined in the RFC 3164 standard. The codes that are applicable to the AT-S63 management software and its modules are shown in Table 7.

Table 7. Default Syslog Facilities

Facility Number	Syslog Protocol Definition	Mapped Event Log Modules and Events
4	Security/ authorization messages	Security and authorization messages from the following modules: DOS, ENCO, PACCESS (802.1x), PKI, PSEC (port security), RADIUS, SSH, SSL, TACACS+, and system events such as user login and logout.
9	Clock daemon	Time-based activities and events from the following modules: TIME, SNTP, and RTC.
16	Local use 0	All other modules and events.
22	Local use 6	Physical interface and data link events from the following modules: PCFG (port configuration), PMIRR (port mirroring), PTRUNK (port trunking), STP, and VLANs.
23	Local use 7	System events related to major exceptions.

For example, the setting of DEFAULT assigns port mirroring events a code of 22 and encryption key events a code of 4.

Another option is to assign all the events the same numerical code using the LOCAL1 to LOCAL7 options. Each option represents a predefined RFC 3164 numerical code. The code mappings are listed in Table 8.

Table 8. Numerical Code and Facility Level Mappings

Numerical Code	Facility Level Setting
17	LOCAL1
18	LOCAL2
19	LOCAL3
20	LOCAL4
21	LOCAL5
22	LOCAL6
23	LOCAL7

For example, selecting LOCAL2 as the facility level assigns the numerical code of 18 to all events sent to the syslog server by the switch.

The SYSLOGFORMAT parameter defines the content of the events.

Examples

The following command creates output definition number 10, sends the messages to a syslog server in normal format with a facility level setting of LOCAL6:

```
create log output=10 destination=syslog server=149.65.10.99
facility=local6 syslog format=normal
```

The following command creates output definition number 18 and sends all of the messages to the syslog server. Because the FORMAT option is omitted from the command, the messages are sent in extended format, which is the default:

```
create log output=18 destination=syslog server=149.65.10.101
```

AlliedWare Plus Command

Syntax

```
log host ipaddress output-id
```

Mode

Configure mode

Description

This AlliedWare Plus command is used to create syslog output definitions. To create a definition, you specify the IP address of a syslog server and a definition ID number. You cannot specify a facility level or a message format. The default values are used for these parameters.

Example

This command creates a new syslog definition. The IP address of the server is 149.24.111.23 and the definition is assigned the ID number 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# log host 149.24.111.23 2
```

DESTROY LOG OUTPUT

AlliedWare Plus Command Available

Syntax

```
destroy log output=output-id
```

Parameters

output Specifies the output definition ID number.

Description

This command deletes output definitions. To disable an output definition without deleting it, see “DISABLE LOG OUTPUT” on page 313.

Example

This command deletes output definition number 3:

```
destroy log output=3
```

AlliedWare Plus Command

Syntax

```
no log host ipaddress output-id
```

Mode

Configure mode

Description

This AlliedWare Plus command is used like the standard command to delete output definitions. It differs from the standard command in that it requires an IP address of a definition’s syslog server.

Example

This command deletes output definition 4. The IP address of the syslog server in the definition is 149.122.45.78:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log host 149.122.45.78 4
```

DISABLE LOG

Syntax

```
disable log
```

Parameters

None.

Description

This command disables the event log module. When the log module is disabled, the AT-S63 management software stops storing events in the event logs and sending events to output definitions. The default setting for the event logs is enabled.

Note
The event log module, even when disabled, still logs all AT-S63 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S63 initialization are recorded only if the event log module is enabled.

Examples

The following command disables the event log on the switch:

```
disable log
```

DISABLE LOG OUTPUT

AlliedWare Plus Command Available

Syntax

```
disable log output[=output-id]
```

Parameters

output	Specifies the output definition ID number to disable. Not specifying an output definition disables all definitions.

Description

This command disables an output definition. When disabled, no event messages are sent to the specified device, although the definition still exists. To permanently remove an output definition, see "DESTROY LOG OUTPUT" on page 311. To enable the output definition again, see "ENABLE LOG OUTPUT" on page 316.

Example

The following command disables (but does not delete) output definition number 7:

```
disable log output=7
```

The following command disables all configured definitions:

```
disable log output
```

AlliedWare Plus Command

Syntax

```
no log enable output-id
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This command disables output definition number 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no log enable 2
```

ENABLE LOG

Syntax

```
enable log
```

Parameters

None.

Description

This command activates the event logs. The switch immediately starts to store the events in the logs and to send the events to the defined outputs. The default setting for the event logs is enabled.

Example

The following command activates the event log module on the switch:

```
enable log
```

ENABLE LOG OUTPUT

AlliedWare Plus
Command
Available

Syntax

```
enable log output[=output-id]
```

Parameters

output	Specifies the output definition ID number to enable. The range is 2 to 20.

Description

This command enables an output definition that was disabled using “DISABLE LOG OUTPUT” on page 313.

Example

The following command enables output definition number 4:

```
enable log output=4
```

The following command enables all output definitions:

```
enable log output
```

AlliedWare Plus Command

Syntax

```
log enable output-id
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This command enables output definition number 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# log enable 2
```

PURGE LOG

AlliedWare Plus Command Available

Syntax

```
purge log[=permanent|temporary]
```

Parameter

log — Specifies the type of memory on the switch where the log file you want to purge is located. The options are:

- permanent — Permanent (nonvolatile) memory. Deletes all events stored in nonvolatile memory, which can contain up to 2,000 events.
- temporary — Temporary memory. Deletes all events stored in temporary memory, which can contain up to 4,000 events. This is the default if you do not specify the “permanent” option.

Description

This command deletes all the entries stored in the event logs.

Example

The following command deletes all the entries in the event log in temporary memory:

```
purge log=temporary
```

The following command deletes all the entries in both event logs:

```
purge log
```

AlliedWare Plus Command

Syntax

```
clear log
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command clears the entries in both the permanent log and the temporary log. There is no AlliedWare Plus command to clear the logs individually.

Example

```
awplus# clear log
```

SAVE LOG

Syntax

```
save log[=permanent|temporary] filename=filename.log [full]
[module=module] [reverse] [severity=all|severity]
[overwrite]
```

Parameters

log Specifies the source of the events you want to save to the log file. The options are:

permanent Permanent (nonvolatile) memory. Saves events stored in nonvolatile memory, which can contain up to 2,000 events.

temporary Temporary memory. Saves events stored in temporary memory, which can contain up to 4,000 events. This is the default.

filename Specifies the filename for the log. The name can be up to 16 alphanumeric characters, followed by the extension ".log." Spaces are allowed. The filename must be enclosed in quotes if it contains spaces. Otherwise, the quotes are optional.

full Specifies the amount of information saved to the log. Without this option, the log saves only the time, module, severity, and description for each entry. With it, the log also saves the filename, line number, and event ID.

module Specifies the AT-S63 module whose events are to be saved. For a list of modules, refer to Table 9 on page 327. Omitting this parameter saves the events from all the modules.

reverse Specifies the order of the events in the log. Without this option, the events are saved oldest to newest. With this option, the events are saved newest to oldest.

severity Specifies the severity of events to be saved. The options are:

all Saves events of all severity levels.

severity Saves events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 329. The default is E, W, I.

overwrite Overwrites the file if it already exists. Without this option, the command displays an error if a file with the same name already exists in the switch’s file system.

Description

This command saves the current entries in an event log to a file in the file system. The parameters in the command allow you to specify which events you want saved in the log file.

Examples

The following command saves the event messages stored in the permanent event log to a file called “switch2.log”. Because the MODULE and SEVERITY parameters are not included in the command, the defaults are used, which is events from all modules with an informational, error, or warning severity level:

```
save log=permanent filename=switch2.log
```

The following command saves the error messages of the VLAN module stored in the temporary event log in a file called “sw14.log.”:

```
save log=temporary filename=sw14.log module=vlan severity=e
```

The following command saves informational messages from all modules in a file called “sw56.log” and overwrites the file of the same name if it already exists in the file system:

```
save log=permanent filename=sw56.log severity=i overwrite
```

SET LOG FULLACTION

Syntax

```
set log fullaction [temporary=halt|wrap]
[permanent=halt|wrap]
```

Parameters

fullaction — Specifies what happens when a log reaches maximum capacity. You can set the action separately for each log. The possible actions are:

halt	The log stops storing new events.
wrap	The log deletes the oldest entries as new ones are added. This is the default.

Description

This command defines the action that an event log takes after it reaches its maximum number of entries. The HALT option instructs a log to stop storing new entries when it reaches its maximum capacity. The WRAP option instructs a log to delete the oldest entries as it adds new entries.

To view the current actions of the event logs, refer to "SHOW LOG OUTPUT" on page 331.

Example

The following command configures the event log in permanent memory to stop storing new entries after it has stored the maximum number of allowed entries:

```
set log fullaction permanent=halt
```

SET LOG OUTPUT

AlliedWare Plus
Command
Available

Syntax

```
set log output=output-id [destination=syslog]
server=ipaddress
[facility=default|local1|local2|local3|local4|local5|local6
|local7] [syslogformat=extended|normal] [module=all|module]
[severity=all|severity-list]
```

Parameters

output
Specifies an ID number that identifies the output definition to be modified. The possible output IDs are:

0
Reserved for permanent (nonvolatile) storage. You cannot change or delete this ID.

1
Reserved for temporary (dynamic) storage. You cannot change or delete this ID.

2 - 20
Available to be used for other outputs.

destination
Specifies the destination for the log messages. The only option currently supported is:

syslog
Forwards log messages in syslog format to a syslog server.

server
Specifies a new IP address for the syslog server.

facility
Specifies a facility level to be added to the events.

default
Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S63 management software and its modules are shown in Table 7 on page 308. This is the default setting.

local1 to local7
Adds a set facility code of 17 (LOCAL1) to 23 (LOCAL7) to all event messages. For a list of the levels and their corresponding codes, refer to Table 8 on page 309.

syslogformat
Specifies the format of the generated messages. The possible options are:

- extended
  Messages include the date, time, and system name. This is the default.
- normal
  Messages do not include the date, time, and system name.

module
Specifies what AT-S63 events to filter. The available options are:

- all
  Sends events for all modules. This is the default.
- module
  Sends events for specific module(s). You can select more than one module at a time, for example, MAC,PACCESS. For a list of modules, see Table 9, “AT-S63 Modules” on page 327.

severity
Specifies the severity of events to be sent. The options are:

- all
  Sends events of all severity levels.
- severity
  Sends events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 329. The defaults are I, E, and W.

Description

This command modifies an existing output definition. For further information on the FACILITY and SYSLOGFORMAT parameters, see “CREATE LOG OUTPUT” on page 306. For further information about the MODULE and SEVERITY parameters, see “ADD LOG OUTPUT” on page 304.

Note
This version of the AT-S63 management software supports only syslog servers as output definitions.

Examples

The following command changes the IP address for output definition number 5 to 149.55.55.55:

```
set log output=5 server=149.55.55.55
```

The following command modifies output definition number 6 to only send messages from the RADIUS module of all severity levels:

```
set log output=6 module=radius severity=all
```

The following command changes the facility level and message format for output definition 4. The facility level is changed to LOCAL1 (numerical code 17) and the format to normal so that the messages include only severity, module, and description:

```
set log output=11 facility=local1 syslogformat=normal
```

The following command changes syslog server definition 11 to send only spanning tree and IGMP snooping events with a severity level of error or warning:

```
set log output=11 module=stp,igmpsnooping severity=e,w
```

AlliedWare Plus Command

Syntax

To set the facility level of an output definition:

```
log monitor facility default|local1|local2|local3|local4|
local5|local6|local7] output-id
```

To define the severity level of the messages of an output definition:

```
log monitor level E|W|I output-id
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is used to set the facility levels and the severity levels of the output definitions. The severity levels are I for Informational, E for Error, and W for Warning, You cannot set any of the other parameters in the standard command with the AlliedWare Plus commands.

Examples

This command sets the facility level on output definition 4 to Local5:

```
awplus> enable
awplus# configure terminal
awplus(config)# log monitor facility local5 4
```

This command sets the severity level on output definition 2 to warning messages:

```
awplus> enable
awplus# configure terminal
awplus(config)# log monitor level w 2
```

SHOW LOG

AlliedWare Plus Command Available

Syntax

```
show log[=permanent|temporary] [full] [module=module]
[reverse] [severity=severity]
```

Parameters

log
Specifies which of the two event logs you want to view. The options are:

- permanent — Displays the events stored in permanent memory.
- temporary — Displays the events stored in temporary memory. This is the default.

full
Specifies the amount of information displayed by the log. Without this option, the log displays the time, module, severity, and description for each entry. With it, the log also displays the filename, line number, and event ID.

module
Specifies the AT-S63 module whose events you want displayed. For a list of modules, refer to Table 9 on page 327.

reverse
Specifies the order of the events in the log. Without this option, the events are displayed oldest to newest. With this option, the events are displayed newest to oldest.

severity
Specifies the severity of events to be displayed. The options are:

- all — Displays events of all severity levels.
- severity — Displays events of a particular severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can select more than one severity at a time (for example, E,W). For a definition of the severity levels, see Table 10, “Event Log Severity Levels” on page 329. The defaults are I, E, and W.

Description

This command displays the entries stored in an event log.

An event log can display entries in two modes: normal and full. In the normal mode, a log displays the time, module, severity, and description for each entry. In the full mode, a log also displays the filename, line number, and event ID. If you want to view the entries in the full mode, use the FULL parameter. To view entries in the normal mode, omit the parameter.

The MODULE parameter displays entries generated by a particular AT-S63 module. You can specify more than one module at a time. If you omit this parameter, the log displays the entries for all the modules. Table 9 lists the modules and their abbreviations.

Table 9. AT-S63 Modules

Module Name	Description
ALL	All modules
ACL	Port access control list
CFG	Switch configuration
CLASSIFIER	Classifiers used by ACL and QoS
CLI	Command line interface commands
DOS	Denial of service defense
ENCO	Encryption keys
ESTACK	Enhanced stacking
EVTLOG	Event log
FILE	File system
GARP	GARP GVRP
HTTP	Web server
IGMPSNOOP	IGMP snooping
IP	System IP configuration
LACP	Link Aggregation Control Protocol
MAC	MAC address table
MGMTACL	Management access control list
MLDSNOOP	MLD snooping
PACCESS	802.1x port-based access control

Table 9. AT-S63 Modules (Continued)

Module Name	Description
PCFG	Port configuration
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	MAC address-based port security
PTRUNK	Static port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
RPS	Redundant power supply
RRP	RRP snooping
RTC	Real time clock
SNMP	SNMP
SSH	Secure Shell protocol
SSL	Secure Sockets Layer protocol
STP	Spanning Tree, Rapid Spanning, and Multiple Spanning Tree protocols
SYSTEM	Hardware status; manager and operator log in and log off events.
TACACS	TACACS+ authentication protocol
TELNET	Telnet
TFTP	TFTP
TIME	System time and SNTP
VLAN	Port-based and tagged VLANs, and multiple VLAN modes
WATCHDOG	Watchdog timer

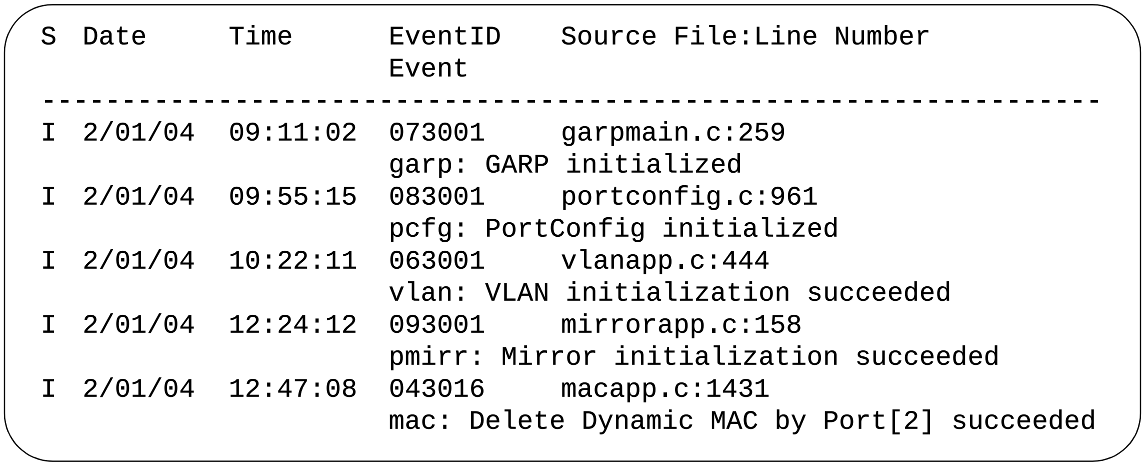
The log can display its entries in chronological order (oldest to newest), or reverse chronological order. The default is chronological order. To reverse the order, use the REVERSE parameter.

The SEVERITY parameter displays entries of a particular severity. Table 10 defines the different severity levels. You can specify more than one severity level at a time. The default is to display error, warning, and informational messages.

Table 10. Event Log Severity Levels

Value	Severity Level	Description
E	Error	Switch operation is severely impaired.
W	Warning	An issue may require manager attention.
I	Informational	Useful information that can be ignored during normal operation.
D	Debug	Messages intended for technical support and software development.

An example of the event log is shown in Figure 51. The example uses the full display mode.



```
S  Date     Time      EventID    Source File:Line Number
                      Event
------------------------------------------------------------------
I  2/01/04  09:11:02  073001     garpmain.c:259
                      garp: GARP initialized
I  2/01/04  09:55:15  083001     portconfig.c:961
                      pcfg: PortConfig initialized
I  2/01/04  10:22:11  063001     vlanapp.c:444
                      vlan: VLAN initialization succeeded
I  2/01/04  12:24:12  093001     mirrorapp.c:158
                      pmirr: Mirror initialization succeeded
I  2/01/04  12:47:08  043016     macapp.c:1431
                      mac: Delete Dynamic MAC by Port[2] succeeded
```

Figure 51. Event Log Example

The columns in the log are described below:

- S (Severity) - The event’s severity. Refer to Table 10 on page 329.
- Date/Time - The date and time the event occurred.
- Event - The module within the AT-S63 software that generated the event followed by a brief description of the event. For a list of the AT-S63 modules, see Table 9 on page 327.
- Event ID - A unique number that identifies the event. (Displayed only in the full display mode.)
- Filename and Line Number - The subpart of the AT-S63 module and the line number that generated the event. (Displayed only in the full display mode.)

Examples

The following command displays all the entries in the event log stored in permanent memory:

```
show log=permanent
```

The following command displays the events stored in temporary memory in the full display mode, which adds more information:

```
show log=temporary full
```

The following command displays only those entries stored in temporary memory and associated with the AT-S63 modules FILE and QOS:

```
show log=permanent module=file,qos
```

The following command displays the error and warning entries for the AT-S63 module VLAN. Because the log is not specified, the temporary log is displayed by default:

```
show log module=vlan severity=e,w
```

AlliedWare Plus Command

Syntax

To display the event messages stored in the permanent event log, from the oldest to the newest messages:

```
show log permanent
```

To display the event messages stored in the temporary event log, from the newest to the oldest messages:

```
show log tail
```

Modes

User Exec mode and Privileged Exec mode

Description

These AlliedWare Plus commands do not have any of the parameters of the standard command.

Examples

To display the events in the permanent log:

```
awplus# show log permanent
```

To display the events in the temporary event log:

```
awplus# show log tail
```

SHOW LOG OUTPUT

AlliedWare Plus Command Available

Syntax

```
show log output[=output-id] [full]
```

Parameters

output Specifies the output definition ID number. If an output ID number is not specified, all output definitions currently configured on the switch are displayed.

full Displays the details of the output definition. If not specified, only a summary is displayed.

Description

This command displays output definition details. An example of the information displayed by this command is shown in Figure 52.

```
OutputID   Type           Status       Details
-----------------------------------------------------------
0          Permanent      Enabled      Wrap on Full
1          Temporary      Enabled      Wrap on Full
2          Syslog         Enabled      169.55.55.55
3          Syslog         Enabled      149.88.88.88
```

Figure 52. SHOW LOG OUTPUT Command

The columns in the display are described below:

- Output ID - The ID number of the output definition. The permanent event log has the ID 0 and the temporary log has the ID 1. Syslog server definitions start with ID 2.
- Type - The type of output definition. Permanent is the permanent event log and Temporary is the temporary event log. Syslog indicates a syslog server definition.
- Status - The status of the output definition, which can be enabled or disabled.
- Details - The event log full action or a syslog server’s IP address. For an event log, this column contains the log’s full action. Wrap on Full indicates that the log adds new entries by deleting old entries when it reaches maximum capacity. Halt on Full means the log stops adding entries after reaching maximum capacity. To configure the full action for an event log, refer to “SET LOG FULLACTION” on page 321. For a syslog definition, this column contains the IP address of the syslog server.

An example of the information displayed by this command with the FULL parameter is shown in Figure 53.

```
Output ID ................... 2
Output Type ................. Syslog
Status ...................... Enabled
Server IP Address ........... 149.88.88.88
Message Format .............. Extended
Facility Level .............. DEFAULT
Event Severity .............. E,W,I
Event Module ................ All
```

Figure 53. SHOW LOG OUTPUT Command with the FULL Parameter

For definitions of the parameters, refer to “SET LOG OUTPUT” on page 322.

Examples

The following command lists all the output definitions:

```
show log output
```

The following command displays the details of output definition number 5:

```
show log output=5 full
```

AlliedWare Plus Command

Syntax

```
show log config
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command lists the current settings of the two event logs and any syslog definitions, and is equivalent to the standard command without the FULL parameter. An example of the information the command displays is shown in Figure 52 on page 331. This command cannot display detailed information about the syslog definitions because it does not have an equivalent parameter for the FULL parameter in the standard command.

Example

```
awplus# show log config
```

SHOW LOG STATUS

Syntax

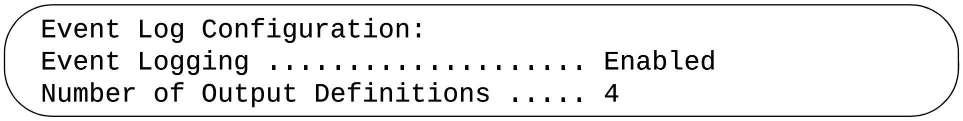
```
show log status
```

Parameter

None.

Description

This command displays information about the event log feature. Figure 54 is an example of the information displayed by this command.



```
Event Log Configuration:
Event Logging .................... Enabled
Number of Output Definitions ..... 4
```

Figure 54. SHOW LOG STATUS Command

The Event Logging field indicates whether the feature is enabled or disabled. If enabled, the switch stores events in the event logs and sends events to defined outputs. If disabled, no events are stored in the event logs or sent to defined outputs. To enable and disable the event logs, refer to “ENABLE LOG” on page 315 and “DISABLE LOG” on page 312.

The Number of Output Definitions is the sum of the two event logs plus any output definitions that you might have created. For instance, the number 4 for Number of Output Definitions in the above example indicates the existence of two output definitions in addition to the two event logs. To create new output definitions, refer to “CREATE LOG OUTPUT” on page 306 and “ADD LOG OUTPUT” on page 304.

Example

The following command displays event log status information:

```
show log status
```

Chapter 18

Classifier Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

CREATE CLASSIFIER

AlliedWare Plus Command Available

Syntax

```
create classifier=idnumber [description="string"]
[macdaddr=macaddress|any] [macsaddr=macaddress|any]
[ethformat=ethii-untagged|ethii-tagged|802.2-
untagged|802.2-tagged|any]
[priority=integer|any] [vlan=name|1..4094|any]
[protocol=ip|arp|rarp|number|any] [iptos=integer|any]
[ipdscp=integer] [ipprotocol=protocol|number|any]
[ipdaddr=ipaddress/mask|any]
[ipsaddr=ipaddress/mask|any] [tcpsport=integer|any]
[tcpdport=integer|any] [udpsport=integer|any]
[udpdport=integer|any]
[tcpflags=[urg|ack|psh|rst|syn|fin|any]
```

Parameters

classifier — Specifies the ID number of the classifier. The number can be from 1 to 9999. Each classifier must have a unique ID number.

description — Specifies a description of up to fifteen alphanumeric characters for the classifier. Spaces are allowed, but a description with spaces must be enclosed in double quotes.

macdaddr — Defines a traffic flow by a destination MAC address. The address can be entered in either of the following formats:

xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

macsaddr — Defines a traffic flow by a source MAC address. The address can be entered in either of the following formats:

xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

ethformat — Defines a traffic flow by the type of Ethernet frame. The options are:

ethII-untagged
ethII-tagged
802.2-untagged
802.2-tagged

priority — Defines a traffic flow by the user priority level in a tagged Ethernet frame. The value can be 0 to 7.

vlan
Defines a traffic flow of a tagged or port-based VLAN by its name or VID number.

protocol
Defines a traffic flow by the protocol specified in the Ethertype field of the MAC header in an Ethernet II frame. Options are:

IP
ARP
RARP

You can specify the protocol by entering the protocol number in either decimal or hexadecimal format. If the latter, precede the number with “0x”. The range is 1536 (0x600) to 65535 (0xFFFF).

iptos
Defines a traffic flow by the Type of Service value. The range is 0 to 7.

ipdscp
Defines a traffic flow by the DSCP value. The range is 0 to 63.

ipprotocol
Defines a traffic flow of a Layer 3 protocol. Options are:

TCP
UDP
ICMP
IGMP

You can specify the protocol by entering the protocol number in either decimal or hexadecimal format. If the latter, precede the number with “0x”. The range is 0 (0x0) to 255 (0xFF).

ipdaddr
Defines a traffic flow by a destination IP address. The address can be of a specific node or a subnet. To filter using the IP address of a subnet, you must include a mask. A mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the subnet address 149.11.11.0 would have a mask of “24” for the twenty-four bits that represent the network section of the address. The address and mask are separated by a slash (/); for example, “IPDADDR=149.11.11.0/24”. No mask is necessary for the IP address of a specific end node.

ipsaddr
Defines a traffic flow by a source IP address. The address can be of a specific node or a subnet. If the latter, a mask must be included to indicate the subnet portion of the address. For an explanation of the mask, refer to the IPDADDR parameter.

tcpsport Defines a traffic flow by a source TCP port.

tcpdport Defines a traffic flow by a destination TCP port.

udpsport Defines a traffic flow by a source UDP port.

udpdport Defines a traffic flow by a destination UDP port.

tcpflags Defines a traffic flow by a TCP flag. Options are

URG - Urgent
ACK - Acknowledgement
RST - Reset
PSH - Push
SYN - Synchronization
FIN - Finish

Description

This command is used to create classifiers. Classifiers define traffic flows for access control lists (ACL) and Quality of Service policies. A traffic flow consists of packets that share one or more characteristics. Traffic flows can range from being very broad to very specific. An example of the former might be all IP traffic while an example of the latter could be packets with specific source and destination MAC addresses.

A classifier without any defined parameters applies to all packets.

The ANY option of the parameters is used to delete the current setting of a parameter without setting a new value.

Examples

This command creates a classifier for all IP traffic:

```
create classifier=4 description=”IP flow” protocol=ip
```

This command creates a classifier for all traffic originating from the subnet 149.22.22.0 destined to the device with the IP address 149.44.44.11:

```
create classifier=4 description=”subnet flow”
ipsaddr=149.22.22.0/24 ipdaddr=149.44.44.11
```

This command creates a classifier for all HTTPS web traffic with a destination IP address of 149.44.44.44:

```
create classifier=7 description=”HTTPS flow”
ipdaddr=149.44.44.44 tcpdport=443
```

AlliedWare Plus Command

To create classifiers with the AlliedWare Plus commands, refer to the AlliedWare Plus sections in “CREATE ACL” on page 348 and “CREATE QOS FLOWGROUP” on page 377.

DESTROY CLASSIFIER

AlliedWare Plus
Command
Available

Syntax

```
destroy classifier=idnumber
```

Parameters

classifier Specifies the ID number of the classifier to be deleted. The number can be from 1 to 9999. You can delete more than one classifier at a time. You can specify the classifiers individually (e.g., 2,5,7) as a range (e.g., 11-14), or both (e.g., 2,4-8,12).

Description

This command deletes classifiers from the switch. To delete a classifier, you need to know its ID number. To display the ID numbers of the classifiers, refer to “SHOW CLASSIFIER” on page 345.

You cannot delete a classifier if it is assigned to an ACL or QoS policy. You have to remove the classifier from the ACL or policy before you can delete it.

Example

This command deletes classifiers 2 and 4:

```
destroy classifier=2,4
```

AlliedWare Plus Command

To delete classifiers with the AlliedWare Plus interface, you delete the access control lists or the flow groups to which they are assigned. For information, refer to the AlliedWare Plus commands in “DESTROY ACL” on page 353 and “DESTROY QOS FLOWGROUP” on page 401.

PURGE CLASSIFIER

Syntax

```
purge classifier
```

Parameters

None.

Description

This command deletes all classifiers from the switch. You cannot delete the classifier if they are assigned to an ACL or QoS policy. You must first remove the classifiers from the ACL and policies before you can delete them.

Example

This command deletes all classifiers on the switch:

```
purge classifier
```

SET CLASSIFIER

Syntax

```
set classifier=idnumber [description="string"]
[macdaddr=macaddress|any] [macsaddr=macaddress|any]
[priority=value] [vlan=name|1..4094|any]
[protocol=ip|arp|rarp|number|any] [iptos=value|any]
[ipdscp=value|any] [ipprotocol=protocol|number|any]
[ipdaddr=ipaddress/mask|any] [ipsaddr=ipaddress/
mask|any] [tcpsport=value|any] [tcpdport=value|any]
[udpsport=value|any] [udpdport=value|any]
[tcpflags=[urg|ack|psh|rst|syn|fin|any]
```

Parameters

classifier
Specifies the ID number of the classifier to be modified. You can modify only one classifier at a time. The number can be from 1 to 9999.

description
Specifies a description of the classifier. A description can be up to fifteen alphanumeric characters. Spaces are allowed. If it contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

macdaddr
Specifies a destination MAC address. The address can be entered in either of the following formats:

xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

macsaddr
Specifies a source MAC address. The address can be entered in either of the following formats:

xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

priority
Specifies the user priority level in a tagged Ethernet frame. The value can be 0 to 7.

vlan
Specifies a tagged or port-based VLAN by its name or VID number.

protocol
Specifies a Layer 2 protocol. Options are:

IP
ARP
RARP

You can specify additional Layer 2 protocols by entering the protocol number in either decimal or hexadecimal format. For the latter, precede the number with “0x”.

iptos Specifies a Type of Service value. The range is 0 to 7.

ipdscp Specifies a DSCP value. The range is 0 to 63.

ipprotocol Specifies a Layer 3 protocol. Options are:

TCP
UDP
ICMP
IGMP

You can specify other Layer 3 protocols by entering the protocol number in either decimal or hexadecimal format. If you use the latter, precede the number with "0x".

ipdaddr Specifies a destination IP address. The address can be of a specific node or a subnet. To filter using the IP address of a subnet, you must include a mask. A mask is a decimal number that represents the number of bits in the address, from left to right, that constitute the network portion of the address. For example, the Class C subnet address 149.11.11.0 would have a mask of "24" for the twenty-four bits that represent the network section of the address. The address and mask are separated by a slash (/); for example, "IPDADDTR=149.11.11.0/24". No mask is necessary for the IP address of a specific end node.

ipsaddr Specifies a source IP address. The address can be of a specific node or a subnet. If the latter, a mask must be included to indicate the subnet portion of the address. For an explanation of the mask, refer to the IPDADDR parameter.

tcpsport Specifies a source TCP port.

tcpdport Specifies a destination TCP port.

udpsport Specifies a source UDP port.

udpdport Specifies a destination UDP port.

tcpflags Specifies a TCP flag. Options are

URG - Urgent
ACK - Acknowledgement
RST - Reset
PSH - Push
SYN - Synchronization
FIN - Finish

Description

This command is used to modify classifiers. You can change all the parameters of a classifier except for the ID number.

Specifying a new value for a variable that already has a value overwrites the current value with the new one. To remove a value from a variable without assigning a new value, use the ANY option.

You cannot modify a classifier if it belongs to an ACL or QoS policy that is assigned to a port. You must first remove the port assignments from the ACL or policy before you can modify it.

Examples

This command adds the destination IP address 149.22.22.22 and the source subnet IP address 149.44.44.0 to classifier ID 4:

```
set classifier=4 ipdaddr=149.22.22.22
ipsaddr=149.44.44.0/24
```

This command adds the Layer 3 protocol IGMP to classifier ID 6:

```
set classifier=6 ipprotocol=igmp
```

This command removes the current setting for the UDP destination port variable from classifier ID 5 without assigning a new value:

```
set classifier=5 udpdport=any
```

SHOW CLASSIFIER

AlliedWare Plus
Command
Available

Syntax

```
show classifier[=idnumber]
```

Parameters

classifier Specifies the ID of the classifier you want to view. You can specify more than one classifier at a time.

Description

This command displays the classifiers on a switch. Figure 55 is an example of the information displayed by this command.

```
---------------------------------------------
Classifier ID: .................. 1
Description: .................... IP traffic
Protocol: ....................... 0x800 (IP)
Number of References: ........... 4
Number of Active Associations: .. 3
---------------------------------------------
Classifier ID: .................. 2
Description: .................... subnet 214
Dst IP/Mask: .................... 169.254.44.214
Number of References: ........... 1
Number of Active Associations: .. 1
---------------------------------------------
```

Figure 55. SHOW CLASSIFIER Command

The information displayed by this command is described here:

- ❒ ID - The classifier's ID number.
- ❒ Description - The description of the classifier.
- ❒ The Description is followed by the parameter settings of the classifier. Only those parameters that have been assigned a value are displayed. For an explanation of the parameters, refer to "CREATE CLASSIFIER" on page 336 or "SET CLASSIFIER" on page 342.
- ❒ Number of References - The number of active and inactive ACL and QoS policy assignments where the classifier is currently assigned. An active ACL or QoS policy is assigned to at least one switch port while an inactive ACL or policy is not assigned to any ports. If this number is 0 (zero), the classifier has not been assigned to any ACLs or policies.

❒ Number of Active Associations - The number of active ACLs and QoS policy assignments where the classifier is currently assigned. An active ACL or policy is assigned to at least one switch port.

You can use this number together with the Number of References to determine the number of inactive ACLs and policies for a classifier. For example, if Number of References for a classifier is 4 and the Number of Active Associations is 3, one of the ACL or QoS policy assignments for the classifier is not assigned to a switch port.

Examples

This command displays all of the classifiers on the switch:

```
show classifier
```

This command displays the details for just classifier ID 12:

```
show classifier=12
```

AlliedWare Plus Command

Syntax

```
show access-list id_number
```

Mode

User Exec mode and Privileged Exec mode

Description

This command displays both the classifiers and the access control lists.

Examples

This command displays all the classifiers and the access control lists:

```
awplus# show access-list
```

This command displays the classifier and the access control list with the ID number 4:

```
awplus# show access-list 4
```

Chapter 19

Access Control List Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

CREATE ACL

AlliedWare Plus
Command
Available

Syntax

```
create acl=value [description="string"]
[action=deny|permit] classifierlist=value
[portlist=ports]
```

Parameters

acl Specifies an ID number for the ACL. The number can be from 0 to 255. Each ACL must have a unique ID number.

description Specifies a description for the ACL. A description can be up to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

action Specifies the action to be taken by the port when a ingress packet matches a classifier attached to the ACL. Options are:

permit The port accepts the packet.

deny The port discards the packet, provided that the packet does not match the classifier of a permit ACL assigned to the same port. This is the default action.

classifierlist Specifies the ID numbers of the classifiers to be assigned to the ACL. When entering multiple ID numbers, separate the numbers with a comma (e.g., 4,6,7). The classifiers must already exist on the switch or stack. The order in which you specify the classifiers is not important. An ACL must have at least one classifier.

portlist Specifies the port for the ACL. An ACL can be assigned to more than one port. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

Description

This command creates access control lists (ACLs), which are used to filter ingress packets on the ports.

Examples

The following command creates an ACL for port 4 that discards the ingress traffic flow specified in classifier ID 18:

```
create acl=12 description=”IP flow deny” action=deny
classifierlist=18 portlist=4
```

The following command creates an ACL that discards the ingress traffic flows specified in classifier ID 2 and 17 and applies the ACL to ports 2 and 6:

```
create acl=6 description=”subnet flow deny”
action=deny classifierlist=2,17 portlist=2,6
```

The following command creates the new ACL 24, which permits on ports 8 to 10 the ingress traffic defined in classifier ID 18:

```
create acl=24 description=”subnet flow deny”
action=permit classifierlist=18 portlist=8-10
```

AlliedWare Plus Command

Syntax

To create access control lists with classifiers that filter ingress packets based on:

❒ Source IP addresses:

```
access-list 1-99 permit|deny ipaddress/mask|any
```

❒ Destination IP addresses:

```
access-list 100-155 permit|deny ipaddress/mask|any
```

❒ IP protocols:

```
access-list 156-199 permit|deny icmp|igmp|tcp|udp
```

❒ Source MAC addresses:

```
access-list 200-255 permit|deny macaddress|any
```

To add access control lists to ports:

```
service-policy access id
```

To remove access control lists from ports:

```
no service-policy access id
```

Modes

For the ACCESS-LIST commands:

Configure mode

For the SERVICE-POLICY ACCESS commands:

Port Interface mode

Description

As explained in the *AT-S63 Management Software Features Guide*, an access control list has two parts. There is the classifier, which defines the traffic flow, and the access control list itself, which defines the action that the ports should take when they receive packets that are members of the defined traffic flow.

The AlliedWare Plus commands handle these elements in very different ways than the other management interfaces. These differences, which are explained here, should be taken into account when deciding whether to use the AlliedWare Plus commands or the other management interfaces to manage this feature.

The classifiers and the access control lists are considered as separate elements by the other management interfaces — the menus, the web browser windows, and the standard command line. To manage this feature with one of these interfaces, you first have to create the classifiers that define the traffic flows you want to control, and then the access control lists that define whether the ports accept or reject the packets of the defined flows.

In contrast, the AlliedWare Plus commands consider an access control list and its classifier as a single unit. You create both at the same time with the ACCESS-LIST commands.

Another difference is how you define the traffic flows. With the other management interfaces, you define the traffic flows by selecting the desired criteria when you create the classifiers.

With the AlliedWare Plus commands the traffic flows are defined by the ID numbers, which are divided into ranges, with each range representing a different criterion. The ID number tells the AlliedWare Plus commands the intended traffic flow of an access control list. For instance, to filter on source IP addresses, you would select an ID number in the range of 1 to 99. Or, for a filter of ICMP packets, you would select an ID number in the range of 156 to 199.

If you look at the description of “CREATE CLASSIFIER” on page 336, you’ll see that classifiers have quite a few criteria for you to choose from in defining traffic flows. But most of the criteria are not available to you when you manage this feature with the AlliedWare Plus commands. You are limited to these four criteria:

- ❒ Source IP addresses
- ❒ Destination IP addresses
- ❒ IP protocols
- ❒ Source MAC addresses

If you are interested in controlling only these flow groups, then you can use the ACCESS-LIST commands to create the access control lists. But if you need to control other flow groups, you'll have to use a different management interface.

Access control lists are not the only feature that use classifiers. Flow groups, which are part of the Quality of Service (QoS) policies, also use them to identify the traffic flows the policies should control. In some situations, you might want access control lists and flow groups to share the same classifier to filter the same traffic. This is possible with the other management interfaces, because you create and manage the classifiers separately from the access control lists and the traffic flows.

But the same isn't true with the AlliedWare Plus commands. Since these commands consider a classifier inseparable from its flow group or access control list, you can't apply the same classifier to more than one flow group or access control list.

Examples

This example configures ports 2 and 4 to accept traffic only from nodes that have source IP addresses in the 149.22.124.0 subnet. The permitted traffic is defined in the classifier and the access control list that are assigned ID number 10. All the other traffic is denied in the classifier and the access control list that are assigned the ID number 30:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 10 permit 149.22.124.0/24
awplus(config)# access-list 30 deny any
awplus(config)# interface 2,4
awplus(config-if)# service-policy access 10
awplus(config-if)# service-policy access 30
```

This example configures port 11 to reject TCP traffic:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 170 deny tcp
awplus(config)# interface 11
awplus(config-if)# service-policy access 170
```

This example removes the access control list 110 from port 22:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22
awplus(config-if)# no service-policy access 110
```

DESTROY ACL

AlliedWare Plus
Command
Available

Syntax

```
destroy acl=id_number
```

Parameters

acl	Specifies ID number of the ACL you want to delete. You can delete more than ACL at a time.

Description

You use this command to delete ACLs. This command does not delete the classifiers of the ACLs. To delete classifiers using the standard command interface, refer to “DESTROY CLASSIFIER” on page 340 or “PURGE CLASSIFIER” on page 341.

Example

The following command deletes ACL IDs 14 and 17:

```
destroy acl=14,17
```

AlliedWare Plus Command

Syntax

```
no access-list id_number
```

Mode

Configure mode

Description

This command has the following rules and restrictions:

- This command deletes both the classifier and its access control list if they have the same ID number. The standard command deletes just the classifier.
- If the classifier and the access control list have different ID numbers, the command deletes just the access control list and displays an error message that the classifier could not be located.
- You should remove the port assignments from the access control list before issuing this command. Otherwise, the command deletes the access control list but not classifier. This rule does not apply to the DESTROY ACL command.

Example

This command deletes the classifier and the access control list with the ID number 5:

```
awplus# no access-list 5
```

PURGE ACL

Syntax

```
purge acl
```

Parameters

None.

Description

This command deletes all the ACLs.

Example

```
purge acl
```

SET ACL

AlliedWare Plus
Command
Available

Syntax

```
set acl=value [description=string]
[action=deny|permit] [classifierlist=value]
[portlist=ports|none]
```

Parameters

acl
: Specifies the ID number of the ACL you want to modify. The number can be from 0 to 255. You can modify only one ACL at a time.

description
: Specifies a new description for the ACL. A description can be up to 15 alphanumeric characters. Spaces are allowed. If the description contains a space, it must be enclosed in double quotes. Otherwise, the quotes are optional.

action
: Specifies the new action to be taken by the port when an ingress packet matches a classifier attached to the ACL. Options are:

permit — The port accepts the packet.

deny — The port discards the packet, provided that the packet does not match the classifier of a permit ACL assigned to the same port.

classifierlist
: Specifies the new ID numbers of the classifiers to be assigned to the ACL. Any classifier IDs already assigned to the ACL are overwritten. When entering multiple ID numbers, separate the numbers with a comma (e.g., 4,6,7). The classifiers must already exist on the switch or stack. The order in which you specify the classifiers is not important. An ACL must be assigned at least one classifier.

portlist
: Specifies the new ports for the ACL. Any ports already assigned to the ACL are overwritten. You can assign the ACL to more than one port. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

Entering NONE removes all ports to which the ACL is already assigned without assigning any new ports. An ACL without assigned ports exists, but remains nonfunctional until assigned to a port.

Description

This command modifies ACLs. You can change the description, action, classifiers, and ports of an ACL.

Examples

This command changes the description of ACL ID 4:

```
set acl=4 description=”ARP flow”
```

This command changes the action of ACL ID 6 to permit and reassigns it to ports 4 to 7:

```
set acl=6 action=permit portlist=4-7
```

This command changes the classifiers of ACL ID 41:

```
set acl=41 classifierlist=22,24,36
```

AlliedWare Plus Command

Syntax

To add access control lists to ports:

```
service-policy access id
```

To remove access control lists from ports:

```
no service-policy access id
```

Mode

Port Interface mode

Description

You use this command to add and remove ports from access control lists. You cannot change the description, the action, or the classifier list of an access control list with the AlliedWare Plus commands.

Example

This example adds port 15 to access control list 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15
awplus(config-if)# service-policy access 5
```

This example removes port 23 from access control list 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 23
awplus(config-if)# no service-policy access 18
```

SHOW ACL

AlliedWare Plus Command Available

Syntax

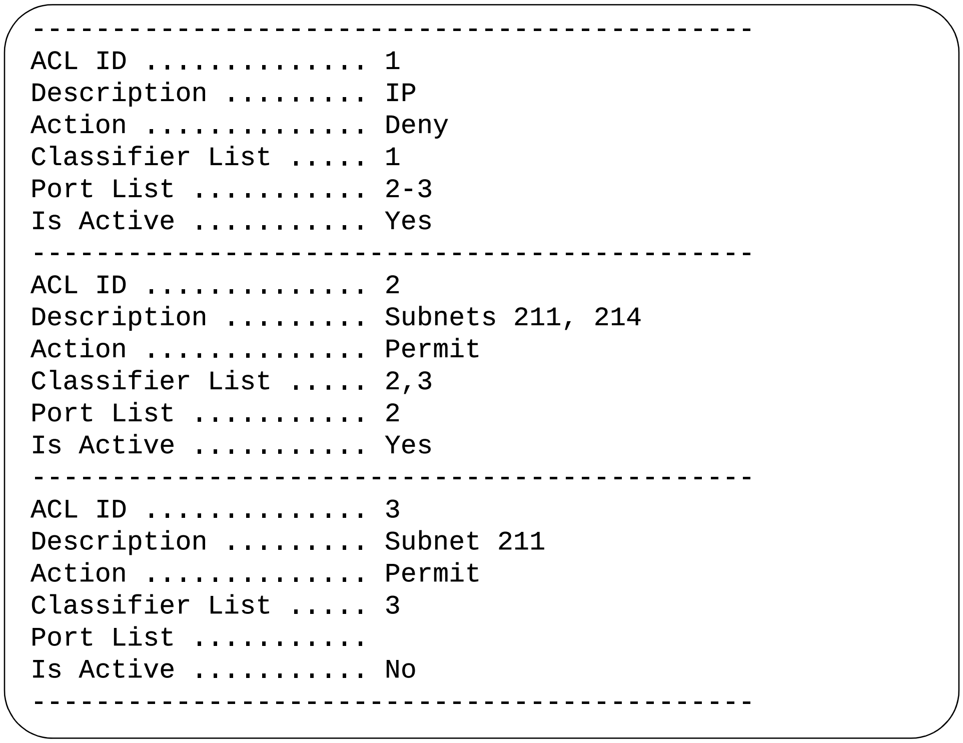
```
show acl[=id_number]
```

Parameters

acl Specifies the ID number of the ACL you want to view. You can specify more than one ACL at a time.

Description

This command displays the ACLs. An example of the information is shown in Figure 56.



```
---------------------------------------------
ACL ID .............. 1
Description ......... IP
Action .............. Deny
Classifier List ..... 1
Port List ........... 2-3
Is Active ........... Yes
---------------------------------------------
ACL ID .............. 2
Description ......... Subnets 211, 214
Action .............. Permit
Classifier List ..... 2,3
Port List ........... 2
Is Active ........... Yes
---------------------------------------------
ACL ID .............. 3
Description ......... Subnet 211
Action .............. Permit
Classifier List ..... 3
Port List ...........
Is Active ........... No
---------------------------------------------
```

Figure 56. SHOW ACL Command

The command displays the following information:

- ACL ID - The ACL’s ID number.
- Description - The description of the ACL.
- Action - The action of the ACL. An active of Permit means that the port(s) where the ACL is assigned accepts those packets that meet the criteria of the classifiers. An action of Deny means that the port(s)

discards the packets provided that the packets do not also meet the criteria of a classifier of a Permit ACL assigned to the same port.

- Classifier List - The classifiers assigned to the ACL.
- Port List - The ports where the ACL is assigned.
- Is Active - The status of the ACL. An ACL is active if it is assigned to at least one port, and inactive if it is not assigned to any ports.

Examples

This command displays all the ACLs:

```
show acl
```

This command displays ACL ID 22:

```
show acl=22
```

AlliedWare Plus Command

Syntax

show access-list *id_number*

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays all the classifiers and the access control lists. The standard command displays just the access control lists.

Examples

This command displays all the classifiers and the access control lists:

```
awplus# show access-list
```

This command displays the classifier and the access control list with the ID number 4:

```
awplus# show access-list 4
```

Chapter 20

Class of Service (CoS) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

MAP QOS COSP

AlliedWare Plus Command Available

Syntax

```
map qos cosp=priority-number qid=queue-number
```

Parameters

cosp Specifies a Class of Service (CoS) priority level. The CoS priority levels are 0 through 7, with 0 as the lowest priority and 7 as the highest. You can specify more than one priority to assign to the same egress queue.

qid Specifies the egress queue number. The egress queues are numbered 0 through 7, with queue 0 as the lowest priority and 7 as the highest.

Description

This command maps CoS priorities to port egress queues. You must specify both the priority and the queue ID. You can specify more than one priority to assign to the same egress queue. Table 11 lists the default mappings between the eight CoS priority levels and the eight egress queues of a switch port.

Table 11. Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q1
1	Q0 (lowest)
2	Q2
3	Q3
4	Q4
5	Q5
6	Q6
7	Q7 (highest)

Example

This command maps priorities 4 and 5, to queue 3:

```
map qos cosp=4,5 qid=3
```

Equivalent Command

```
set qos cosp=priority-number qid=queue-number
```

For information, see "SET QOS COSP" on page 365.

AlliedWare Plus Command

Syntax

```
mls qos map cos-queue priority-number queue-number
```

or

```
no mls qos map cos-queue priority-number queue-number
```

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This command maps priorities 1 and 2 to queue 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# mls qos map cos-queue 1,2 5
```

PURGE QOS

Syntax

```
purge qos
```

Parameters

None

Description

This command destroys all policies, traffic classes, and flow groups; resets the CoS priorities to port egress queues to the default values; and sets the scheduling mode and egress weight queues to their default values.

Example

The following command resets QoS to the default values:

```
purge qos
```

SET QOS COSP

AlliedWare Plus Command Available

Syntax

```
set qos cosp=priority-number qid=queue-number
```

Parameters

cosp	Specifies a Class of Service (CoS) priority level. The CoS priority levels are 0 through 7, with 0 as the lowest priority and 7 as the highest. You can specify more than one priority to assign to the same egress queue.
qid	Specifies the egress queue number. The egress queues are numbered 0 through 7, with queue 0 as the lowest priority and 7 as the highest.

Description

This command maps CoS priorities to port egress queues. You must specify both the priority and the queue ID. You can assign more than one priority to an egress queue. Table 11 on page 362 lists the default mappings between the eight CoS priority levels and the eight egress queues of a switch port.

Example

The following command maps priorities 5 and 6 to egress queue 1:

```
set qos cosp=5,6 qid=1
```

Equivalent Command

```
map qos cosp=priority-number qid=queue-number
```

For information, see “MAP QOS COSP” on page 362.

AlliedWare Plus Command

For the equivalent AlliedWare Plus command, refer to the AlliedWare Plus Command section in “MAP QOS COSP” on page 362.

SET QOS SCHEDULING

AlliedWare Plus
Command
Available

Syntax

```
set qos scheduling=strict|wrr weights=weights
```

Parameters

scheduling
Specifies the type of scheduling. The options are:

strict
Strict priority. The port transmits all packets out of the higher priority queues before it transmits any from the low priority queues. This is the default.

wrr
Weighted round robin. The port transmits a set number of packets from each queue in a round robin manner.

weights
Specifies the weights given to a port’s eight egress priority queues. You must specify the weights if scheduling will be weighted round robin. The range for Q0 to Q6 is 1 to 15 packets. The range for Q7 is 0 to 15 packets. A setting of 0 for Q7 means that its packets always take priority over the packets in the other queues, and that packets are transmitted from the other queues only when Q7 is empty.

The weights are specified in the following order: Q0, Q1, Q2, Q3, Q4, Q5, Q6, Q7. For example, to assign Q0 and Q1 a weight of 1, Q2 and Q3 a weight of 5, Q4 and Q5 a weight of 10, and Q6 and Q7 a weight of 15, you enter this parameter as:

```
weights=1,1,5,5,10,10,15,15
```

You must specify all eight queues.

The default setting for all the queues is 1, meaning that all the queues have the same weight.

Description

Sets the QoS scheduling method and the weights for round robin scheduling.

Examples

This command sets the scheduling to strict:

```
set qos scheduling=strict
```

This command sets the scheduling to weighted round robin and gives egress priority queues Q0 to Q3 a weight of 1, and Q4 to Q7 a weight of 15:

```
set qos scheduling=wrr weights=1,1,1,1,15,15,15,15
```

AlliedWare Plus Command

Syntax

To set the scheduling method to strict priority:

```
mls qos strict
```

or

```
no mls qos strict
```

To set the scheduling method to weighted round robin:

```
wrr-queue weight weights
```

Mode

Configure mode

Description

These AlliedWare Plus command are equivalent to the standard command.

Example

This example sets the scheduling to strict priority:

```
awplus> enable
awplus# configure terminal
awplus(config)# mls qos strict
```

This example sets the scheduling to weighted round robin and gives egress priority queues Q0 and Q1 a weight of 1, Q2 and Q3 a weight of 10, and Q4 to Q7 a weight of 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# wrr-queue weight 1,1,10,10,15,15,15,15
```

SET SWITCH PORT PRIORITY OVERRIDEPRIORITY

AlliedWare Plus
Command
Available

Syntax

```
set switch port=port [priority=value]
[overridepriority=yes|no|on|off|true|false]
```

Parameters

port	Specifies the port you want to configure. You can specify more than one port at a time, but the ports must be of the same medium type. For example, you cannot configure twisted pair and fiber optic ports with the same command. For instructions, refer to “Port Numbers in Commands” on page 48.
priority	Specifies a temporary priority level for all ingress untagged packets received on a port. If you include the OVERRIDEPRIORITY parameter, the temporary priority level will also apply to all ingress tagged packets. The range is 0 to 7; 0 is the lowest priority, and 7 is the highest. The default is 0.Table 11 on page 362 lists the default mappings between the priority levels and the egress queues:
overridepriority	Determines whether a port should ignore the priority level in tagged packets and instead use the temporary priority level assigned to the port with the PRIORITY parameter. The options are:

yes, on, true	Overrides the priority level in tagged packets and uses the temporary priority level. This is the default. The options are equivalent.
no, off, false	Does not override the priority in tagged packets. The options are equivalent.

Description

This command can change a port’s temporary priority level. It can also be used to determine whether a port receiving tagged packets should use the priority level in the frames or instead use a temporary priority level assigned to the port.

This command allows you to override the priority level mappings at the port level by assigning the packets a temporary priority. Note that this assignment is made when a packet is received on the ingress port and before the frame is forwarded to the egress port. Consequently, you need to configure this feature on the ingress port.

For example, you can configure a switch port so that all ingress frames are assigned a temporary priority level of 5, regardless of the actual priority levels that might be in the frames themselves, as found in tagged frames.

A temporary priority level applies only while a frame traverses the switching matrix. Tagged frames, which can contain a priority level, leave the switch with the same priority level they had when they entered the switch.

Examples

This command assigns the temporary priority level of 5 to ports 5, 8, and 12:

```
set switch port=5,8,12 priority=5
```

This command activates the priority override feature on port 6 so that all ingress tagged packets use the port’s temporary priority level:

```
set switch port=6 overridepriority=yes
```

AlliedWare Plus Command

Syntax

To specify a temporary priority level for the ingress packets on a port:

```
priority-queue value
```

To specify whether or not a port should ignore the priority level in tagged packets:

```
override-priority enable|disable
```

Mode

Interface mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This example assigns a priority level of 3 to port 4 and activates the priority override feature:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 4
awplus(config-if)# priority-queue 3
awplus(config-if)# override-priority enable
```

SHOW QOS CONFIG

AlliedWare Plus
Command
Available

Syntax

```
show qos config
```

Parameters

None.

Description

Displays the CoS priority queues and scheduling. Figure 57 is an example of the information displayed by this command.

```
QoS Configuration information:

Number of CoS Queues .......... 8

CoS 0 Priority Queue .......... Q1
CoS 1 Priority Queue .......... Q0
CoS 2 Priority Queue .......... Q2
CoS 3 Priority Queue .......... Q3
CoS 4 Priority Queue .......... Q4
CoS 5 Priority Queue .......... Q5
CoS 6 Priority Queue .......... Q6
CoS 7 Priority Queue .......... Q7


Scheduling Mode ............... Strict Priority
Queue 0 Weight ................ 0
Queue 1 Weight ................ 0
Queue 2 Weight ................ 0
Queue 3 Weight ................ 0
Queue 4 Weight ................ 0
Queue 5 Weight ................ 0
Queue 6 Weight ................ 0
Queue 7 Weight ................ 0
```

Figure 57. SHOW QOS CONFIG Command

The current mapping of CoS priorities to port egress queues is displayed in the top section. As an example, at the default setting packets with a CoS priority of 3 are stored in egress queue 3 of a port.

The bottom section of the display shows the scheduling method of the switch ports. In strict priority, a port transmits all packets out of the higher priority queues before transmitting any from the low priority queues. This is the default. In weighted round robin, a port transmits a set number of packets from each queue. The weights only show a value when a port is using weighted round robin and specify how many packets a port transmits from a queue before moving to the next queue.

Example

The following command displays the CoS priority queues and scheduling:

```
show qos config
```

AlliedWare Plus Command

Syntax

```
show mls qos cos-queue
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
show mls qos cos-queue
```

Chapter 21

Quality of Service (QoS) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD QOS FLOWGROUP

Syntax

```
add qos flowgroup=value classifierlist=values
```

Parameter

flowgroup Specifies the ID number of the flow group you want to modify. You can modify only one flow group at a time.

classifierlist Specifies the new classifiers for the flow group. The new classifiers are added to any classifiers already assigned to the flow group. Separate multiple classifiers with commas (e.g., 4,11,12).

Description

This command adds classifiers to existing flow groups. The classifiers must already exist. Any classifiers already assigned to the flow groups are retained by the groups. If you want to add classifiers while removing the those already assigned, refer to “SET QOS FLOWGROUP” on page 406.

Example

This command adds the classifiers 4 and 7 to flow group 12:

```
add qos flowgroup=12 classifierlist=4,7
```

ADD QOS POLICY

Syntax

```
add qos policy=value trafficclasslist=values
```

Parameter

policy — Specifies the ID number of the policy you want to modify. You can modify only one policy at a time.

trafficclasslist — Specifies the new traffic classes of the policy. Traffic classes already assigned to the policy are retained. Separate multiple traffic classes with commas (e.g., 4,11,12).

Description

This command adds traffic classes to an existing policy. The traffic classes must already exist. Any traffic classes already assigned to the policy are retained by the policy. To add traffic classes while removing those already assigned, refer to "SET QOS POLICY" on page 409.

Example

This command adds the traffic class 16 to policy 11:

```
add qos policy=11 trafficclasslist=16
```

ADD QOS TRAFFICCLASS

Syntax

```
add qos trafficclass=value flowgrouplist=values
```

Parameter

trafficclass — Specifies the ID number of the traffic class you want to modify. You can modify only one traffic class at a time.

flowgrouplist — Specifies the new flow groups of the traffic class. The new flow groups are added to any flow groups already assigned to the flow group. Separate multiple flow groups with commas (e.g., 4,11,12).

Description

This command adds flow groups to existing traffic classes. The flow groups must already exist. Any flow groups already assigned to a traffic class are retained by the class. If you want to add flow groups while removing those already assigned, refer to “SET QOS TRAFFICCLASS” on page 414.

Examples

This command adds flow group 21 to traffic class 17:

```
add qos trafficclass=17 flowgrouplist=21
```

CREATE QOS FLOWGROUP

AlliedWare Plus
Command
Available

Syntax

```
create qos flowgroup=value [description=”string”]
[markvalue=value|none] [priority=value|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[classifierlist=values|none]
```

Parameters

flowgroup

Specifies an ID number for the flow group. Each flow group on the switch must have a unique number. The range is 0 to 1023. The default is 0. This parameter is required.

description

Specifies a description for the flow group. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. This parameter is optional, but recommended. Names can help you identify the groups on the switch. The description must be enclosed in double quotes if it contains spaces. Otherwise, the quotes are optional.

markvalue

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. If the NONE option is used, the frame’s current DSCP value is not overwritten. The default is NONE.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.

priority

Specifies a new user priority value for the packets. The range is 0 to 7. If you want packets to retain the new value when they exit the switch, use the REMARKPRIORITY parameter. If the NONE option is used, the frame’s current priority value is not overridden. The default is NONE.

A new priority can be set at both the flow group and traffic class levels. If it is set in both places, the value in the flow group overrides the value in the traffic class.

remarkpriority Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter. This parameter is ignored if the PRIORITY parameter is omitted or set to NONE. Options are:

yes, on, true Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter.

no, off, false Does not replace the user priority value in the packets with the new value specified in with the PRIORITY parameter. This is the default.

tos Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes, on, true Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no, off, false Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no, off, false Does not replace the ToS priority field. This is the default.

classifierlist Specifies the classifiers to be assigned to the flow group. Separate multiple classifiers with commas (e.g., 4,7,8). The classifiers must already exist.

Description

This command is used to create new flow groups.

Note
For examples of the command sequences used to create entire QoS policies, refer to “CREATE QOS POLICY” on page 384.

Examples

This command creates a flow group with an ID of 10 and a description of “VoIP flow”. The flow group is assigned a priority level of 7 and defined by classifiers 15 and 17. In this example, the packets of the flow group leave the switch with the same priority level as when they entered. The new priority level is relevant only as the packets traverse the switch. To alter the packets so that they leave containing the new level, you would include the REMARKPRIORITY parameter:

```
create qos flowgroup=10 description=”VoIP flow”
priority=7 classifierlist=15,17
```

This command creates a similar flow group as in the previous example. The REMARKPRIORITY parameter is added so that the tagged packets of the flow group leave the switch with the new priority level of 7:

```
create qos flowgroup=10 description=”VoIP flow”
priority=7 remarkpriority=yes classifierlist=15,17
```

This command creates a flow group whose DSCP value is changed to 59. The MARKVALUE parameter overwrites the current DSCP value in the packets, meaning the packets leave the switch with the new value. The classifiers of the flow group are 3, 14, and 24:

```
create qos flowgroup=10 description=”DSCP 59 flow”
markvalue=59 classifierlist=3,14,24
```

AlliedWare Plus Command

Syntax

Group 1: To create flow groups with classifiers that filter ingress packets based on:

- Source IP addresses:

```
class-map 256-1023
match access-group 1-99
```

- Destination IP addresses:

```
class-map 256-1023
match access-group 100-155
```

- IP protocols:

  ```
  class-map 256-1023
  match access-group 156-199
  ```

- Source MAC addresses:

  ```
  class-map 256-1023
  match access-group 200-255
  ```

Group 2: To create flow groups with classifiers that filter ingress packets based on:

- IP Type of Service values:

  ```
  class-map 256-1023
  match ip-precedence 0-7
  ```

- 802.1p priority values:

  ```
  class-map 256-1023
  match cos 0-7
  ```

- IP DSCP values:

  ```
  class-map 256-1023
  match ip-dscp 0-63
  ```

- TCP flags:

  ```
  class-map 256-1023
  match tcp-flags urg|ack|rst|psh|syn|fin
  ```

- VAN ID values:

  ```
  class-map 256-1023
  match vlan 1-4094
  ```

Mode

Class Map mode

Description

These are the AlliedWare Plus commands for Quality of Service flow groups. They are divided into two groups because of a significant difference between them. The commands in the first group are similar to the standard command in that the classifiers, which define the traffic flows of the policies, have to be created separately, whereas the commands in the second group create the classifiers for you. This difference and others are described here. To better understand this discussion, you should review the background information on classifiers and Quality of Service policies in the *AT-S63 Management Software Features Guide* before you read this description.

Classifiers are an important component of Quality of Service policies because they define the traffic flows of the policies. Classifiers have a host of variables that you can choose from. You might, for instance, create classifiers that define traffic flows based on source or destination IP addresses, IP protocols, or Ethernet frame types.

To create policies with the other management interfaces, you have to create the classifiers separately and afterwards add them to the flow groups. For instance, to create classifiers from the standard command line interface you use the CREATE CLASSIFIER command, described in "CREATE CLASSIFIER" on page 336.

The AlliedWare Plus commands in the first group operate in the same fashion in that the classifiers have to be created separately from the flow groups. To use these commands, you first have to create the classifiers. However, if you've read the description of the CREATE CLASSIFIER command, you'll see there isn't an equivalent AlliedWare Plus command that creates classifiers. So how do you create classifiers for use with the commands in the first group?

You have two choices. First, you can use a different management interface, such as the standard command line and the CREATE CLASSIFIER command. After creating the classifiers, you can enter the AlliedWare Plus command interface and create the flow groups, specifying the classifiers created in the other management interface.

Another way is to use the AlliedWare Plus ACCESS-LIST command. You use this command to create access control lists to control what packets a port accepts or rejects. But access control lists also use classifiers. What you can do is create access control lists using the AlliedWare Plus commands and then add their classifiers to the flow groups. This is demonstrated in Examples later in this section.

The flow group commands in the second group create the classifiers for you. For instance, the MATCH TCP-FLAGS command creates a classifier containing the specified TCP flag.

The AlliedWare Plus commands have other differences from the standard commands. If you examine the syntax of "CREATE CLASSIFIER" on page 336, you'll see that there are a wide range of variables for defining traffic flows. But the AlliedWare Plus commands support only a subset of the possible variables. For instance, to create policies for packets containing defined TCP or UDP port values, you' have to use the standard commands or another management interface, because the AlliedWare Plus commands do not support those classifier criteria.

The same restrictions apply to the variables within the flow groups themselves. If you examine the syntax of the standard CREATE QOS

FLOWGROUP command, you'll see that there are different actions that the flow group can perform, such as replacing values in the Type of Service or priority fields of the packets. These parameters are not available in the AlliedWare Plus commands. In fact, the only parameters you can control in policies created with the AlliedWare Plus commands are the maximum bandwidth value and the replacement DSCP value, set when you create the traffic classes.

Here are a few other differences between the AlliedWare Plus commands and the other management interfaces:

- Flow groups created with the other management interfaces can have more than one classifier, making it possible to create policies that control more than one traffic flow. In contrast, flow groups created with the AlliedWare Plus commands can control only one traffic flow because they can have only one classifier.
- You can use the other management interfaces to modify Quality of Service policies created with the AlliedWare Plus commands. But the reverse isn't true. That is you cannot use the AlliedWare Plus commands to modify policies created with one of the other interfaces.

Group 1 Examples

This example creates a classifier and a flow group for packets with the source IP address 149.11.14.0. The classifier is created with the AlliedWare Plus ACCESS-LIST command and is assigned the ID number 2. The flow group is given the ID number 270. This example starts at the User Exec mode in the AlliedWare Plus command interface:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 2 permit 149.11.14.0/24
awplus(config)# class-map 270
awplus(config-cmap)# match access-group 2
```

You notice an action of Permit in the ACCESS-LIST command. The action pertains to the access control list and not to the classifier. If the access control list will not be used, the action can be either Permit or Deny.

This example is the same as the previous one, except the standard CREATE CLASSIFIER command is used to create the classifier. It starts at the standard command line prompt:

```
# create classifier=2 ipsaddr=149.11.14.0/24
# awplus
awplus> enable
awplus# configure terminal
awplus(config)# class-map 270
awplus(config-cmap)# match access-group 2
```

This example creates a classifier and a flow group for TCP packets. The classifier is created with the AlliedWare Plus ACCESS LIST command and is assigned the ID number 182. Since The flow group is assigned the ID number 271. This example starts at the User Exec mode in the AlliedWare Plus command interface:

```
awplus> enable
awplus# configure terminal
awplus(config)# access-list 182 permit tcp
awplus(config)# class-map 271
awplus(config-cmap)# match access-group 182
```

This example, which starts at the standard command line prompt, is the same as the previous one, except the standard CREATE CLASSIFIER command is used to create the classifier:

```
# create classifier=270 ipprotocol=tcp
# awplus
awplus> enable
awplus# configure terminal
awplus(config)# class-map 270
awplus(config-cmap)# match access-group 2
```

Group 2 Examples

This example creates a classifier and a flow group for packets with an IP Type of Service value of 5. The classifier and flow group are assigned the ID number 265:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map 265
awplus(config-cmap)# match ip-precedence 5
```

This example creates a classifier and a flow group for packets with an IP DSCP value of 55. The classifier and flow group are assigned the ID number 270:

```
awplus> enable
awplus# configure terminal
awplus(config)# class-map 270
awplus(config-cmap)# match ip-dscp 55
```

CREATE QOS POLICY

AlliedWare Plus Command Available

Syntax

```
create qos policy=value [description=“string”]
[indscpoverwrite=value|none] [remarkindscp=all|none]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[sendtomirror=yes|no|on|off|true|false]
[trafficclasslist=values|none]
[redirectport=value|none]
[ingressport=port|all|none] [egressport=port|none]
```

Parameters

policy
Specifies an ID number for the policy. Each policy on the switch must be assigned a unique number. The range is 0 to 255. The default is 0. This parameter is required.

description
Specifies a description for the policy. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional. This parameter is optional, but recommended. Names can help you identify the policies on the switch.

indscpoverwrite
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. If None is specified, the DSCP value in the packets is not changed. The default is None.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.

remarkindscp
Specifies whether the DSCP value in ingress packets is overwritten. If All is specified, all packets are remarked. If None is specified, the function is disabled. The default is None.

tos
Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes, on, true Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no, off, false Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no, off, false Does not replace the ToS priority field. This is the default.

sendtomirror Copies the traffic that meets the criteria of the classifiers to a destination mirror port. Options are:

yes, on, true Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by creating a port mirror, as explained in Chapter 13, "Port Mirroring Commands" on page 237.

no, off, false Does not copy the traffic to a destination mirror port. This is the default.

trafficclasslist Specifies the traffic classes to be assigned to the policy. The specified traffic classes must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

redirectport Specifies the port to which the classified traffic from the ingress ports is redirected. The options are:

value Specifies a port number.

none No redirect port specified.

ingressport

Specifies the ingress ports for the policy. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

A port can be an ingress port of only one policy at a time. If a port is already an ingress port of a policy, you must remove the port from its current policy assignment before adding it to another policy.

egressport

Specifies the egress port to which the policy is to be assigned. You can enter only one egress port. The egress port must be within the same port block as the ingress ports. On switches with 24 ports (plus uplinks), ports 1-26 form a port block. On switches with 48 ports (plus uplinks), ports 1-24 and 49 form one port block and ports 25-48 and 50 form a second port block.

A port can be an egress port of only one policy at a time. If a port is already an egress port of a policy, you must remove the port from its current policy assignment before adding it to another policy.

Description

This command is used to create new QoS policies.

Examples

This command creates a policy with an ID of 75 and the description “DB flow.” The policy is appointed the traffic classes 12 and 25 and is assigned to ingress port 5:

```
create qos policy=75 description=”DB flow”
trafficclasslist=12,25 ingressport=5
```

This command creates a policy with an ID of 23 and the description “Video.” The ID of the traffic class for the policy is 19. The DSCP value is replaced with the value 50 for all ingress packets of the traffic class. The policy is assigned to port 14:

```
create qos policy=23 description=video
indscpoverwrite=50 remarkindscp=all
trafficclasslist=19 ingressport=14
```

QoS Command Sequence Examples

To create a QoS policy you have to create one or more classifiers, a flow group, a traffic class, and finally the policy. The following sections contain examples of the command sequences for different types of policies.

Example 1: Voice Application

Voice applications typically require a small bandwidth but it must be consistent. They are sensitive to latency (interpacket delay) and jitter (delivery delay). Voice applications can be set up to have the highest priority.

This example creates two policies that ensure low latency for all traffic sent by and destined to a voice application located on a node with the IP address 149.44.44.44. The policies raise the priority level of the packets to 7, the highest level. Policy 6 is for traffic from the application that enter the switch on port 1. Policy 11 is for traffic arriving on port 8 going to the application.

Policy 6 Commands:

```
create classifier=22 description=”VoIP flow”
ipsadddr=149.44.44.44
```

```
create qos flowgroup=14 description=”VoIP flow”
priority=7 classifierlist=22
```

```
create qos trafficclass=18 description=”VoIP flow”
flowgrouplist=14
```

```
create qos policy=6 description=”VoIP flow”
trafficclasslist=18 ingressport=1
```

Policy 11 Commands:

```
create classifier=23 description=”VoIP flow”
ipdadddr=149.44.44.44
```

```
create qos flowgroup=17 description=”VoIP flow”
priority=7 classifierlist=23
```

```
create qos trafficclass=15 description=”VoIP flow”
flowgrouplist=17
```

```
create qos policy=11 description=”VoIP flow”
trafficclasslist=15 ingressport=8
```

The parts of the policies are:

- ❒ Classifiers - Define the traffic flow by specifying the IP address of the node with the voice application. The classifier for Policy 6 specifies the address as a source address since this classifier is part of a policy concerning packets coming from the application. The classifier for Policy 11 specifies the address as a destination address since this classifier is part of a policy concerning packets going to the application.
- ❒ Flow Groups - Specify the new priority level of 7 for the packets. It should be noted that in this example the packets leave the switch with the same priority level they had when they entered. The new priority level is relevant only as the packets traverse the switch. To alter the packets so that they leave containing the new level, you would use the REMARKPRIORITY option in the CREATE QOS FLOWGROUP command.
- ❒ Traffic Classes - No action is taken by the traffic classes, other than to specify the flow groups. Traffic class has a priority setting that can be used to override the priority level of packets, just as in a flow group. If you enter a priority value both in the flow group and the traffic class, the value in the flow group overrides the value in the traffic class.
- ❒ Policies - Specify the traffic class and the port to which the policy is to be assigned. Policy 6 is applied to port 1 since this is where the application is located. Policy 11 is applied to port 8 since this is where traffic going to the application will be received on the switch.

Example 2: Video Application

Video applications typically require a larger bandwidth than voice applications. Video applications can be set up to have a high priority and buffering, depending on the application.

This example creates policies with low latency and jitter for video streams (for example, net conference calls). The policies assign the packets a priority level of 4. The policies also limit the bandwidth for the video streams to 5 Mbps to illustrate how you can combine a change to the priority level with bandwidth restriction to further define traffic control. The node containing the application has the IP address 149.44.44.44. Policy 17 is assigned to port 1, where the application is located, and Policy 32 is assigned to port 8 where packets destined to the application enter the switch.

Policy 17 Commands:

```
create classifier=16 description=”video flow”
ipsadddr=149.44.44.44

create qos flowgroup=41 description=”video flow”
priority=4 classifierlist=16
```

```
create qos trafficclass=19 description=”video flow”
maxbandwidth=5 flowgrouplist=41
```

```
create qos policy=17 description=”video flow”
trafficclasslist=19 ingressport=1
```

Policy 32 Commands:

```
create classifier=42 description=”video flow”
ipdadddr=149.44.44.44
```

```
create qos flowgroup=36 description=”video flow”
priority=4 classifierlist=42
```

```
create qos trafficclass=21 description=”video flow”
maxbandwidth=5 flowgrouplist=36
```

```
create qos policy=32 description=”video flow”
trafficclasslist=21 ingressport=8
```

The parts of the policies are:

- Classifiers - Specify the IP address of the node with a video application. The classifier for Policy 17 specifies the address as a source address since this classifier is part of a policy concerning packets sent by the application. The classifier for Policy 32 specifies the address as a destination address since this classifier is part of a policy concerning packets going to the application.
- Flow Groups - Specify the new priority level of 4 for the packets. As with the previous example, the packets leave the switch with the same priority level they had when they entered. The new priority level is relevant only while the packets traverse the switch. To alter the packets so that they leave containing the new level, you would change option 5, Remark Priority, to Yes.
- Traffic Classes - Specify a maximum bandwidth of 5 Mbps for the packet stream. Bandwidth assignment can only be made at the traffic class level.
- Policies - Specify the traffic class and the port where the policy is to be assigned.

Example 3: Critical Database

Critical databases typically require a high bandwidth. They also typically require less priority than either voice or video.

The policies in this example assign 50 Mbps of bandwidth, with no change to priority, to traffic going to and from a database. The database is located on a node with the IP address 149.44.44.44 on port 1 of the switch.

Policy 15 Commands:

```
create classifier=42 description=database
ipsadddr=149.44.44.44
```

```
create qos flowgroup=36 description=database
classifierlist=42
```

```
create qos trafficclass=21 description=database
maxbandwidth=50 flowgrouplist=36
```

```
create qos policy=15 description=database
trafficclasslist=21 ingressport=1
```

Policy 17 Commands:

```
create classifier=10 description=database
ipdadddr=149.44.44.44
```

```
create qos flowgroup=12 description=database
classifierlist=10
```

```
create qos trafficclass=17 description=database
maxbandwidth=50 flowgrouplist=12
```

```
create qos policy=17 description=database
trafficclasslist=17 ingressport=8
```

AlliedWare Plus Command

Syntax

service-policy input *id_number*

Mode

Port Interface mode

Description

This AlliedWare Plus command is used to create Quality of Service policies. To use the command, you first enter the Port Interface mode for the ports to be assigned the policy. You then enter this command, using the ID_NUMBER variable to identify the ID number of the traffic class for the policy. The command automatically creates the policy, assigning it the same ID number as the traffic class, and attaches the policy to the ports, which are considered ingress ports of the policy.

If you examine the standard “CREATE QOS POLICY” on page 384, you’ll see that policies actually have quite a few parameters. However, most of them are not available to you when you create policies with this AlliedWare Plus command. The only two parameters that you can set are the ingress ports, which, as just explained, you identify with the Port

Interface mode, and the policy’s traffic class, which you identify with the ID_NUMBER parameter.

Examples

This example creates a new Quality of Service policy on ports 2 and 5. The traffic class for the policy has the ID number 12. Since policies created with the AlliedWare Plus commands are given the same ID numbers as their traffic classes, the policy is also assigned the ID number 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2,5
awplus(config-if)# service-policy input 12
```

CREATE QOS TRAFFICCLASS

AlliedWare Plus Command Available

Syntax

```
create qos trafficclass=value [description="string"]
[exceedaction=drop|remark]
[exceedremarkvalue=value|none] [markvalue=value|none]
[maxbandwidth=value|none] [burstsize=value|none]
[priority=value|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[flowgrouplist=values|none]
```

Parameters

trafficclass
Specifies the ID number for the new flow group. Each flow group must be assigned a unique number. The range is 0 to 511. The default is 0. This parameter is required.

description
Specifies a description for the traffic class. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. This parameter is optional, but recommended. Names can help you identify the traffic classes on the switch.

exceedaction
Specifies the action to be taken if the traffic of the traffic class exceeds the maximum bandwidth, specified with the MAXBANDWIDTH parameter. There are two possible exceed actions, drop and remark. If drop is selected, traffic exceeding the bandwidth is discarded. If remark is selected, the packets are forwarded after replacing the DSCP value with the new value specified by Exceed Remark Value. The default is drop.

exceedremarkvalue
Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value set with the MARKVALUE parameter. The range is 0 to 63. The default is 0.

markvalue
Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.

maxbandwidth

Specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum rate at which the ingress port accepts data belonging to this traffic class before either dropping or remarking occurs, depending on the EXCEEDACTION parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified. The range is 0 to 1016 Mbps.

The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16).

burstsize

Specifies the size of a token bucket for the traffic class. The token bucket is used in situations where you have set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded.

Tokens are added to the bucket at the same rate as the traffic class’ maximum bandwidth, set with the MAXBANDWIDTH parameter. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at that rate.

If the amount of the traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic will be discarded since no tokens are available for handling the increase.

If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded.

Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added. The range is 4 to 512 Kbps.

This parameter must be used with the MAXBANDWIDTH parameter. Specifying a token bucket size without also specifying a maximum bandwidth serves no function.

priority

Specifies the priority value in the IEEE 802.1p tag control field of the traffic specified by the traffic class. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of eight Class of Service (CoS) queues based on the priority value.

If you want the packets to retain the new value when they exit the switch, use the REMARKPRIORITY parameter.

A new priority can be set at both the flow group and traffic class levels. If it is set in both places, the value in the flow group overrides the value in the traffic class.

remarkpriority

Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter. This parameter is ignored if the PRIORITY parameter is omitted or set to NONE. Options are:

yes, on, true — Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter.

no, off, false — Does not replace the user priority value in the packets with the new value specified in with the PRIORITY parameter. This is the default.

tos — Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets. Options are:

yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field in IPv4 packets.

no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field in IPv4 packets.

no, off, false — Does not replace the ToS priority field. This is the default.

flowgrouplist — Specifies the flow groups to be assigned to the traffic class. The specified flow groups must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

Description

This command is used to create new traffic classes.

Note
For examples of the command sequences for entire QoS policies, refer to "CREATE QOS POLICY" on page 384.

Examples

The following command creates a traffic class with an ID number of 25 and the description “Database flow”. The flow group of the traffic class has the ID 11:

```
create qos trafficclass=25 description=”Database flow”
flowgrouplist=11
```

This command creates a traffic class with the ID number of 41 and description “Video flow”. The traffic class is assigned the flow group 3 and is given a maximum bandwidth of 5 Mbps:

```
create qos trafficclass=41 description=”Video flow”
maxbandwidth=5 flowgrouplist=3
```

This command creates a traffic class with the ID number of 51 and description “DB Eng”. It assigns flow group 5 a maximum bandwidth of 50 Mbps. The DSCP value in all flow traffic that exceeds the maximum bandwidth is changed to 35:

```
create qos trafficclass=51 description=”DB Eng”
exceedaction=remark exceedremarkvalue=35
maxbandwidth=50 flowgrouplist=5
```

AlliedWare Plus Command

Syntax

To create a traffic class:

```
policy-map 0-255
```

To map a flow group to a traffic class:

```
class 256-1023
```

To configure the traffic class parameters:

```
set bandwidth 0-1016

set dscp 0-63

set exceed-action drop|remark

set exceed-remark-value 0-63

set burstsize 4-512

set priority 0-7

set remark-priority enable|disable

set tos 0-7
set tos-priority enable|disable
```

```
set priority-tos enable|disable
```

Mode

To create a traffic class:

Configure mode

To map a flow group to a traffic class:

Policy Map mode

To configure the traffic class parameters:

Class mode

Description

These commands have the following restrictions:

- The flow group must already exist.
- You cannot use the AlliedWare Plus commands to modify existing traffic classes. Instead, use "SET QOS TRAFFICCLASS" on page 414 or another management interface.

Example

This example creates a new traffic class with the ID number 11. The ID number of the flow group for the traffic class is 274. The traffic class is assigned a maximum bandwidth of 750 Mbps:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map 11
awplus(config-pmap)# class 274
awplus(config-pmap-c)# set bandwidth 750
```

This example creates a traffic class for a flow group that has the ID number 302. The traffic class is assigned the ID number 12. The traffic class sets the priority of the packets of the traffic flow to 7 and enables the remark option so that the packets retain the new value when they exit the switch:

```
awplus> enable
awplus# configure terminal
awplus(config)# policy-map 12
awplus(config-pmap)# class 302
awplus(config-pmap-c)# set priority 7
awplus(config-pmap-c)# set remark-priority enable
```

DELETE QOS FLOWGROUP

Syntax

```
delete qos flowgroup=value classifierlist=values
```

Parameter

flowgroup	Specifies the ID number of the flow group you want to modify. You can modify only one flow group at a time.

classifierlist	Specifies the classifiers you want to remove from the flow group. Separate multiple classifiers with commas (e.g., 4,11,12). (The online help for this command includes a NONE option for this parameter. Specifying the NONE option does not remove any classifiers. Since the purpose of this command is to remove classifiers from flow groups, you are unlikely ever to use that option.)

Description

This command removes classifiers from flow groups.

Example

This command removes classifier 6 from flow group 22:

```
delete qos flowgroup=22 classifierlist=6
```

DELETE QOS POLICY

Syntax

```
delete qos policy=value trafficclasslist=values
```

Parameter

policy — Specifies the ID number of the policy you want to modify. You can modify only one policy at a time.

trafficclasslist — Specifies the IDs of the traffic classes you want to remove from the policy. Separate multiple traffic class with commas (e.g., 4,11,12). (The online help for this command includes a NONE option for this parameter. Specifying the NONE option does not remove any traffic classes. Since the purpose of this command is to remove traffic classes from a policy, it is unlikely you would ever use that option.)

Description

This command removes traffic classes from policies.

Example

This command removes traffic class 17 from policy 1:

```
delete qos policy=1 trafficclasslist=17
```

DELETE QOS TRAFFICCLASS

Syntax

```
delete qos trafficclass=value flowgrouplist=values
```

Parameter

flowgroup Specifies the ID number of the traffic class you want to modify. You can modify only one traffic class at a time.

flowgrouplist Specifies the IDs of the flow groups you want to remove from the traffic class. Separate multiple flow groups with commas (e.g., 4,11,12). (The online help for this command includes a NONE option for this parameter. Specifying the NONE option does not remove any flow groups. Since the purpose of this command is to remove flow groups from a traffic class, it is unlikely you would ever use that option.)

Description

This command removes flow groups from traffic classes.

Example

This command removes flow group 5 from traffic class 22:

```
delete qos trafficclass=22 flowgrouplist=5
```

DESTROY QOS FLOWGROUP

AlliedWare Plus Command Available

Syntax

```
destroy qos flowgroup=id_number
```

Parameter

flowgroup	Specifies the ID number of the flow group you want to delete. You can delete more than one flow group at a time. You can specify the flow groups individually, as a range, or both.

Description

This command deletes flow groups.

Examples

This command deletes the flow group 22:

```
destroy qos flowgroup=22
```

This command deletes the flow groups 16 to 20 and 23:

```
destroy qos flowgroup=16-20,23
```

AlliedWare Plus Command

Syntax

```
no class-map id_number
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This command deletes flow groups 3 and 4:

```
no class-map 3,4
```

DESTROY QOS POLICY

AlliedWare Plus
Command
Available

Syntax

```
destroy qos policy=value
```

Parameter

flowgroup	Specifies the ID number of the policy you want to delete. You can delete more than one policy at a time. You can specify the flow groups individually, as a range, or both.

Description

This command deletes QoS policies.

Examples

This command deletes policy 41:

```
destroy qos policy=41
```

This command deletes policies 5 and 23:

```
destroy qos policy=5,23
```

AlliedWare Plus Command

Syntax

```
no service-policy input id_number
```

Mode

Port Interface mode

Description

You delete policies with this AlliedWare Plus command by removing all of their ingress ports.

Example

This example removes policy 12 by removing its ingress ports 1 to 4:

```
awplus> enable
awplus# configure terminal
awplus(conf)# interface 1-4
awplus(conf-if)# no service-policy input 12
```

DESTROY QOS TRAFFICCLASS

AlliedWare Plus Command Available

Syntax

```
destroy qos trafficclass=id_number
```

Parameter

trafficclass Specifies the ID number of the traffic class you want to delete. You can delete more than one traffic class at a time. You can specify the flow groups individually, as a range, or both.

Description

This command deletes traffic classes.

> **Note**
> A traffic class must be removed from all of its policy assignments before you can delete it.

Examples

This command deletes traffic class 22:

```
destroy qos trafficclass=22
```

This command deletes traffic classes 16 to 20 and 23:

```
destroy qos trafficclass=16-20,23
```

AlliedWare Plus Command

Syntax

```
no policy-map id_number
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

These commands delete traffic class 5:

```
awplus> enable
awplus# configure terminal
awplus(conf)# no policy-map 5
```

PURGE QOS

Syntax

```
purge qos
```

Parameters

None

Description

This command destroys all the policies, traffic classes, and flow groups; resets the CoS priorities to port egress queues to the default values; and sets the scheduling mode and egress weight queues to their default values.

Example

The following command resets QoS to the default values:

```
purge qos
```

SET QOS FLOWGROUP

Syntax

```
set qos flowgroup=value [description=string]
[markvalue=value|none] [priority=value|NONE]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[classifierlist=values|none]
```

Parameters

flowgroup — Specifies the ID number of the flow group you want to modify. The range is 0 to 1023.

description — Specifies a new description for the flow group. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. This parameter is optional, but recommended. Names can help you identify the groups on the switch. The description must be enclosed in double quotes if it contains spaces. Otherwise, the quotes are optional.

markvalue — Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63. If the NONE option is used, the frame's current DSCP value is not overwritten. The default is NONE.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level.

priority — Specifies a new user priority value for the packets. The range is 0 to 7. You can specify only one value. If you want packets to retain the new value when they exit the switch, use the REMARKPRIORITY parameter. If the NONE option is used, the frame's current priority value is not overridden The default is NONE.

If you specify a new priority in a flow group and a traffic class, the value in the flow group overrides the value in the traffic class.

remarkpriority — Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter. This parameter is ignored if the PRIORITY parameter is omitted or set to NONE.

Options are:

yes, on, true   Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter.

no, off, false   Does not replace the user priority value in the packets with the new value specified in with the PRIORITY parameter. This is the default.

tos   Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority   Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes, on, true   Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no, off, false   Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos   Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true   Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no, off, false   Does not replace the ToS priority field. This is the default.

classifierlist   Specifies the classifiers to be assigned to the flow group. The specified classifiers replace any classifiers already assigned to the flow group. Separate multiple classifiers with commas (e.g., 4,7,8). The classifiers must already exist. The NONE options removes all classifiers currently assigned to the flow group without assigning any new ones. To add classifiers without replacing those already assigned, see “ADD QOS FLOWGROUP” on page 374.

Description

This command modifies the specifications of an existing flow group. The only parameter you cannot change is a flow group's ID number. To initially create a flow group, refer to "CREATE QOS FLOWGROUP" on page 377.

> **Note**
> For examples of command sequences used to create entire QoS policies, refer to "CREATE QOS POLICY" on page 384.

When modifying a flow group, note the following:

- You cannot change a flow group's ID number.
- Specifying an invalid value for a parameter that already has a value causes the parameter to revert to its default value.

Examples

This command changes the user priority value to 6 in flow group 15:

```
set qos flowgroup=15 priority=6
```

This command assigns classifiers 23 and 41 to flow group 25. Any classifiers already assigned to the flow group are replaced:

```
set qos flowgroup=25 classifierlist=23,41
```

This command returns the MARKVALUE setting in flow group 41 back to the default setting of NONE. At this setting, the flow group will not overwrite the ToS setting in the packets:

```
set qos flowgroup=41 markvalue=none
```

SET QOS POLICY

Syntax

```
set qos policy=value [description=string]
[indscpoverwrite=value|none] [remarkindscp=[all|none]]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[sendtomirror=yes|no|on|off|true|false]
[trafficclasslist=values|none]
[redirectport=value|none] [ingressport=port|all|none]
[egressport=port|none]
```

Parameters

policy Specifies an ID number for the policy. Each policy on the switch must be assigned a unique number. The range is 0 to 255. The default is 0. This parameter is required.

description Specifies a description for the policy. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional. This parameter is optional, but recommended. Names can help you identify the policies on the switch.

indscpoverwrite Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.

remarkindscp Specifies the conditions under which the ingress DSCP value is overwritten. If All is specified, all packets are remarked. If None is specified, the function is disabled. The default is None.

tos Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes, on, true Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no, off, false Does not replace the preexisting 802.1p priority level This is the default.

moveprioritytotos Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no, off, false Does not replace the ToS priority field. This is the default.

sendtomirror Copies the traffic that meets the criteria of the classifiers to a destination mirror port. Options are:

yes, on, true Copies the traffic that meets the criteria of the classifiers to a destination mirror port. You must specify the destination port by creating a port mirror, as explained in Chapter 13, “Port Mirroring Commands” on page 237.

no, off, false Does not copy the traffic to a destination mirror port. This is the default.

trafficclasslist Specifies the traffic classes to be assigned to the policy. The specified traffic classes must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

redirectport Specifies the port to which the classified traffic from the ingress ports is redirected.

ingressport Specifies the ingress ports for the policy. For instructions on how to enter the ports, refer to “Port Numbers in Commands” on page 48. To remove all of the current ingress ports, use the NONE option. To add all of the ports as ingress ports, use the ALL option.

The ports specified by this parameter replace any ingress ports already assigned to the policy. To retain the current ingress ports, use the "SET QOS PORT" on page 413 instead of this command to add ingress ports to the policy.

A port can be an ingress port of only one policy at a time. If a port is already an ingress port of a policy, you must remove the port from its current policy assignment before adding it to another policy. Alternatively, you can use "SET QOS PORT" on page 413, which removes a port from a policy and adds it to another policy with one command.

egressport Specifies the egress port to which the policy is to be assigned. You can enter only one egress port. The NONE option removes the policy from all egress ports to which it has been assigned. The ALL option adds it to all ports.

The ports specified by this parameter replace any egress ports already assigned to the policy. To retain the ports, use the "SET QOS PORT" on page 413 instead of this command to add egress ports to the policy.

A port can be an egress port of only one policy at a time. If a port is already an egress port of a policy, you must remove the port from its current policy assignment before adding it to another policy. Alternatively, you can use "SET QOS PORT" on page 413, which removes a port from a policy and adds it to another policy with one command.

Description

This command modifies an existing policy. To initially create a policy, refer to "CREATE QOS POLICY" on page 384.

Note
For examples of command sequences used to create entire QoS policies, refer to "CREATE QOS POLICY" on page 384.

When modifying a policy, note the following:

❒ You cannot change a policy's ID number.

❒ Specifying an invalid value for a parameter that already has a value causes the parameter to revert to its default value.

Examples

This command changes the ingress port for policy 8 to port 23:

```
set qos policy=8 ingressport=8
```

This command changes the traffic classes assigned to policy 41:

```
set qos policy=41 trafficclasslist=12,23
```

SET QOS PORT

Syntax

```
set qos port=value type=ingress|egress
policy=value|none
```

Parameter

port Specifies the port to be added to or removed from a policy. A policy can have more than one ingress port, but only one egress port. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

type Specifies whether the port is an ingress or egress port for the policy. The default is ingress.

policy Specifies the policy to the assigned to the port. You can specify only one policy. The NONE option removes the port from its current policy assignment.

Description

This command adds and removes ports from policies.

A port can be an ingress or egress port of only one policy at a time. However, a port can be an ingress port and an egress port of different policies, simultaneously. If a port is already a port of a policy, this command automatically removes it from its current policy assignment before adding it to another policy.

Examples

This command assigns ports 5 through 8 as ingress ports in QoS policy 12:

```
set qos port=5-8 type=ingress policy=12
```

This command removes egress port 5 from its current policy assignment without assigning it to another policy:

```
set qos port=5 type=egress policy=none
```

SET QOS TRAFFICCLASS

Syntax

```
set qos trafficclass=value [description="string"]
[exceedaction=drop|remark]
[exceedremarkvalue=value|none] [markvalue=value|none]
[maxbandwidth=value|none] [burstsize=value|none]
[priority=value|none]
[remarkpriority=yes|no|on|off|true|false]
[tos=value|none]
[movetostopriority=yes|no|on|off|true|false]
[moveprioritytotos=yes|no|on|off|true|false]
[flowgrouplist=values|none]
```

Parameters

trafficclass
Specifies an ID number for the flow group. Each flow group on the switch must be assigned a unique number. The range is 0 to 511. The default is 0. This parameter is required.

description
Specifies a description for the traffic class. The description can be from 1 to 15 alphanumeric characters. Spaces are allowed. If the description contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional. This parameter is optional, but recommended. Names can help you identify the traffic classes on the switch.

exceedaction
Specifies the action to be taken if the flow group of the traffic class exceeds the maximum bandwidth, specified with the MAXBANDWIDTH parameter. There are two possible exceed actions, drop and remark. If drop is selected, traffic exceeding the bandwidth is discarded. If remark is selected, the packets are forwarded after replacing the DSCP value with the new value specified with the EXCEEDREMARKVALUE parameter. The default is drop.

exceedremarkvalue
Specifies the DSCP replacement value for traffic that exceeds the maximum bandwidth. This value takes precedence over the DSCP value set with the MARKVALUE parameter. The range is 0 to 63. The default is 0.

markvalue

Specifies a replacement value to write into the DSCP (TOS) field of the packets. The range is 0 to 63.

A new DSCP value can be set at all three levels: flow group, traffic class, and policy. A DSCP value specified in a flow group overrides a DSCP value specified at the traffic class or policy level. A DSCP value specified at the traffic class level is used only if no value has been specified at the flow group level. It will override any value set at the policy level.

maxbandwidth

Specifies the maximum bandwidth available to the traffic class. This parameter determines the maximum rate at which the ingress port accepts data belonging to this traffic class before either dropping or remarking occurs, as specified with the EXCEEDACTION parameter. If the sum of the maximum bandwidth for all traffic classes on a policy exceeds the (ingress) bandwidth of the port to which the policy is assigned, the bandwidth for the port takes precedence and the port discards packets before they can be classified. The range is 0 to 1016 Mbps.

The value for this parameter is rounded up to the nearest Mbps value when this traffic class is assigned to a policy on a 10/100 port, and up to the nearest 8 Mbps value when assigned to a policy on a gigabit port (for example, on a gigabit port, 1 Mbps is rounded to 8 Mbps, and 9 is rounded to 16).

burstsize

Specifies the size of a token bucket for the traffic class. The token bucket is used in situations where you have set a maximum bandwidth for a class, but where traffic activity may periodically exceed the maximum. A token bucket can provide a buffer for those periods where the maximum bandwidth is exceeded.

Tokens are added to the bucket at the same rate as the traffic class’ maximum bandwidth, set with the MAXBANDWIDTH parameter. For example, a maximum bandwidth of 50 Mbps adds tokens to the bucket at that rate.

If the amount of the traffic flow matches the maximum bandwidth, no traffic is dropped because the number of tokens added to the bucket matches the number being used by the traffic. However, no unused tokens will accumulate in the bucket. If the traffic increases, the excess traffic will be discarded since no tokens are available for handling the increase.

If the traffic is below the maximum bandwidth, unused tokens will accumulate in the bucket since the actual bandwidth falls below the specified maximum. The unused tokens will be available for handling excess traffic should the traffic exceed the maximum bandwidth. Should an increase in traffic continue to the point where all the unused tokens are used up, packets will be discarded.

Unused tokens accumulate in the bucket until the bucket reaches maximum capacity, set by this parameter. Once the maximum capacity of the bucket is reached, no extra tokens are added. The range is 4 to 512 Kbps.

This parameter should be used with the MAXBANDWIDTH parameter. Specifying a token bucket size without also specifying a maximum bandwidth serves no function.

priority

Specifies the priority value in the IEEE 802.1p tag control field that traffic belonging to this traffic class is assigned. Priority values range from 0 to 7 with 0 being the lowest priority and 7 being the highest priority. Incoming frames are mapped into one of eight Class of Service (CoS) queues based on the priority value.

If you want the packets to retain the new value when they exit the switch, change option 9, Remark Priority, to Yes.

If you specify a new priority in a flow group and a traffic class, the value in the flow group overrides the value in the traffic class.

remarkpriority

Replaces the user priority value in the packets with the new value specified with the PRIORITY parameter, if set to Yes. If set to No, which is the default, the packets retain their preexisting priority level when they leave the switch.

tos

Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.

A new ToS value can be set at all three levels: flow group, traffic class, and policy. A ToS value specified in a flow group overrides a ToS value specified at the traffic class or policy level.

movetostopriority — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. Options are:

yes, on, true — Replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets.

no, off, false — Does not replace the preexisting 802.1p priority level This is the default.

movepriorityto tos — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets. Options are:

yes, on, true — Replaces the value in the ToS priority field with the 802.1p priority field on IPv4 packets.

no, off, false — Does not replace the ToS priority field. This is the default.

flowgrouplist — Specifies the flow groups to be assigned to the traffic class. Any flow groups already assigned to the traffic class are replaced. The specified flow groups must already exist. Separate multiple IDs with commas (e.g., 4,11,13).

Description

This command modifies an existing traffic class. To initially create a traffic class, refer to “CREATE QOS TRAFFICCLASS” on page 392. The only parameter you cannot change is a traffic classes ID number.

> **Note**
> For examples of command sequences used to create entire QoS policies, refer to “CREATE QOS POLICY” on page 384.

When modifying a traffic class, note the following:

- You cannot change a traffic class’ ID number.
- Specifying an invalid value for a parameter that already has a value causes the parameter to revert to its default value.

Examples

This command changes the exceed action in traffic class 18 to remark and specifies a remark value of 24. This command changes the DSCP value in traffic that exceeds the maximum bandwidth to 24:

```
set qos trafficclass=18 exceedaction=remark
exceedremarkvalue=24
```

This command changes the user priority value to 17 for traffic belonging to traffic class 42:

```
set qos trafficclass=42 priority=17
```

This command changes the maximum bandwidth for traffic class 41 to 80 Mbps and the burst size to 400 Kbps.

```
set qos trafficclass=41 maxbandwidth=80 burstsize=400
```

SHOW QOS FLOWGROUP

AlliedWare Plus Command Available

Syntax

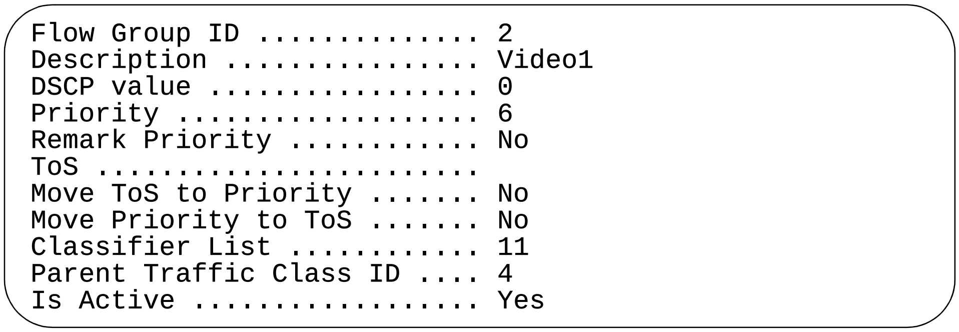
```
show qos flowgroup[=idnumber]
```

Parameters

flowgroup Specifies the ID of the flow group you want to view. You can specify more than one classifier at a time.

Description

This command displays the flow groups on a switch. An example is shown in Figure 58.



```
Flow Group ID ............. 2
Description ................ Video1
DSCP value ................ 0
Priority .................. 6
Remark Priority ........... No
ToS .......................
Move ToS to Priority ....... No
Move Priority to ToS ....... No
Classifier List ........... 11
Parent Traffic Class ID .... 4
Is Active ................. Yes
```

Figure 58. SHOW QOS FLOWGROUP Command

The command displays the following information about a flow group:

- Flow Group ID - The flow group's ID number.
- Description - The flow group's description.
- DSCP value - The replacement value to write into the DSCP (TOS) field of the packets.
- Priority - The new user priority value for the packets.
- Remark Priority - Replaces the user priority value in the packets with the Priority value.
- ToS - Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.
- Move ToS to Priority - If set to Yes, replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting 802.1p priority level.
- Move Priority to ToS - If set to Yes, replaces the value in the ToS priority field with the value in the 802.1p priority field on IPv4 packets. If

set to No, which is the default, the packets retain their preexisting ToS priority level.

- ❐ Classifier List - The classifiers assigned to the policy.
- ❐ Parent Traffic Class ID - The ID number of the traffic class to which the flow group is assigned. A flow group can belong to only one traffic class at a time.
- ❐ Is Active - The status of the flow group. If the flow group is part of a QoS policy that is assigned to one or more ports, the flow group is deemed active. If the flow group has not been assigned to a policy or if the policy has not been assigned to any ports, the flow group is considered inactive.

For further information about the parameters, refer to “CREATE QOS FLOWGROUP” on page 377.

Examples

This command displays all of the flow groups:

```
show qos flowgroup
```

This command displays flow group 12:

```
show qos flowgroup=12
```

AlliedWare Plus Command

Syntax

show class-map [*id_number*]

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Examples

This command displays the details of all the flow groups:

```
awplus# show class-map
```

This command displays the flow group with the ID number 270:

```
awplus# show class-map 270
```

SHOW QOS POLICY

AlliedWare Plus Command Available

Syntax

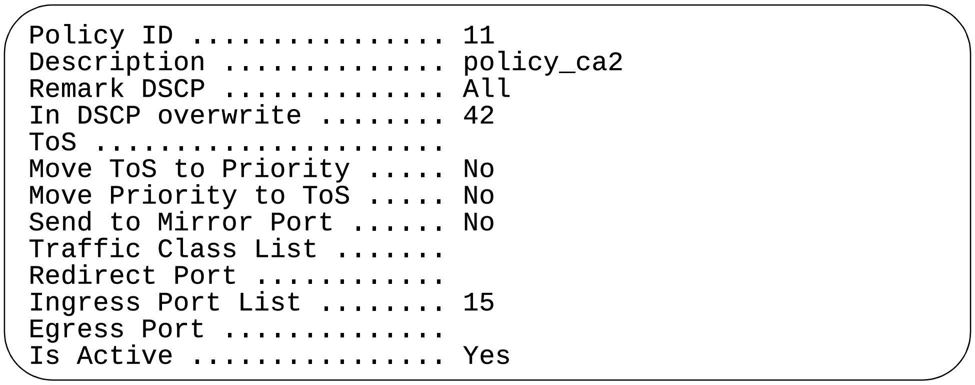
`show qos policy[=`*`idnumber`*`]`

Parameter

policy Specifies the ID of the policy you want to view. You can specify more than one policy at a time. Separate multiple policies with commas (e.g., 4,5,10).

Description

This command displays the policies on a switch. An example is shown in Figure 59.



```
Policy ID ................ 11
Description .............. policy_ca2
Remark DSCP .............. All
In DSCP overwrite ........ 42
ToS ......................
Move ToS to Priority ..... No
Move Priority to ToS ..... No
Send to Mirror Port ...... No
Traffic Class List .......
Redirect Port ............
Ingress Port List ........ 15
Egress Port ..............
Is Active ................ Yes
```

Figure 59. SHOW QOS POLICY Command

This command provides the following information:

- Policy ID - The policy’s ID number.
- Description - The policy’s description.
- Remark DSCP - Specifies whether the DSCP value of ingress packets is overwritten. If All is specified, all packets are remarked. If None is specified, the function is disabled. The default is None.
- In DSCP overwrite - The replacement value to write into the DSCP (TOS) field of the packets.
- ToS - Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7. A ToS value specified at the policy level is used only if no value has been specified at the flow group and traffic class levels.
- Move ToS to Priority - If set to yes, replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. If

set to No, which is the default, the packets retain their preexisting 802.1p priority level.

- Move Priority to ToS - If set to yes, replaces the value in the ToS priority field with the value in the 802.1p priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting ToS priority level.
- Send to Mirror Port - Copies the traffic that meets the criteria of the classifiers to a destination mirror port. If set to yes, you must specify the destination port of the port mirror with “SET SWITCH MIRROR” on page 238.
- Traffic Class List - The traffic classes assigned to the policy.
- Redirect Port - The egress port to which the classified traffic from the ingress port is reassigned.
- Ingress Port List - The ingress ports to which the policy is assigned.
- Egress Port - The egress port to which the policy is assigned.
- Active - The status of the policy. A policy that is assigned to one or more ports is deemed active while a policy that is not assigned to any ports is deemed inactive.

For further information about the parameters, refer to “CREATE QOS POLICY” on page 384.

Examples

This command displays all of the policies:

```
show qos policy
```

This command displays policy 54:

```
show qos policy=54
```

AlliedWare Plus Command

Syntax

show service-policy [*id_number*]

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Examples

This command displays the details of all the policies:

```
awplus# show service-policy
```

This command displays policy 4:

```
awplus# show service-policy 4
```

SHOW QOS TRAFFICCLASS

AlliedWare Plus Command Available

Syntax

show qos trafficclass[=*idnumber*]

Parameter

trafficclass	Specifies the ID of the traffic class you want to view. You can specify more than one traffic class at a time. Separate multiple traffic classes with commas (e.g., 4,5,10).

Description

This command displays the traffic classes on a switch. An example is shown in Figure 60.

```
Traffic Class ID .......... 0
Description ............... Dev Database
Exceed Action ............. Drop
Exceed Remark Value ....... 0
DSCP value ................ 0
Max bandwidth ............. 50
Burst Size ................ 0
Priority .................. 0
Remark Priority ........... No
ToS .......................
Move ToS to Priority ...... No
Move Priority to ToS ...... No
Flow Group List ........... 11
Parent Policy ID .......... 2
Is Active ................. Yes
```

Figure 60. DISPLAY QOS TRAFFICCLASS Command

This command provides the following information about a traffic class:

- ❐ Traffic Class ID - The traffic class’ ID number.
- ❐ Description - The description of the traffic class.
- ❐ Exceed Action - The action taken if the traffic of the traffic class exceeds the maximum bandwidth.
- ❐ Exceed Remark Value - The DSCP replacement value for traffic that exceeds the maximum bandwidth.
- ❐ DSCP value - The replacement value to write into the DSCP (TOS) field of the packets.
- ❐ Max Bandwidth - The maximum bandwidth available to the traffic class.
- ❐ Burst Size - The size of a token bucket for the traffic class.

- Priority - The priority value in the IEEE 802.1p tag control field assigned to the traffic that belongs to this traffic class.
- Remark Priority - Replaces the user priority value in the packets with the Priority value.
- ToS - Specifies a replacement value to write into the Type of Service (ToS) field of IPv4 packets. The range is 0 to 7.
- Move ToS to Priority - If set to yes, replaces the value in the 802.1p priority field with the value in the ToS priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting 802.1p priority level.
- Move Priority to ToS - If set to yes, replaces the value in the ToS priority field with the value in the 802.1p priority field on IPv4 packets. If set to No, which is the default, the packets retain their preexisting ToS priority level.
- Flow Group List - The flow groups assigned to the traffic class.
- Parent Policy ID - The ID number of the policy where the traffic class is assigned. A traffic class can belong to only one policy at a time.
- Is Active - The status of the traffic class. If the traffic class is part of a QoS policy that is assigned to one or more ports, the traffic class is deemed active. If the traffic class has not been assigned to a policy or if the policy has not been assigned to any ports, the traffic class is deemed inactive.

For further information about the parameters, refer to “CREATE QOS TRAFFICCLASS” on page 392.

Examples

This command displays all of the traffic classes:

```
show qos trafficclass
```

This command displays traffic class 14:

```
show qos trafficclass=14
```

AlliedWare Plus Command

Syntax

```
show policy-map [id_number]
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Examples

This command displays the details of all the traffic classes:

```
awplus# show policy-map
```

This command displays the traffic class with the ID number 12:

```
awplus# show policy-map 12
```

Chapter 22

Group Link Control Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD GLC

AlliedWare Plus Command Available

Syntax

```
add glc upstream|downstream group port
```

Parameters

upstream| downstream	Specifies whether a port is to be an upstream port or a downstream port of a group.
group	Specifies a group for a port. You can specify only one group and the group must already exist. The range is 1 to 8.
port	Specifies a port to add to a group. You can specify more than one port.

Description

This command is used to add upstream and downstream ports to groups for group link control. Here are the guidelines:

- ❒ A group must already exist before you can add ports to it. To create groups, refer to "CREATE GLC" on page 430.
- ❒ You can add either upstream ports or downstream ports to a group, but not both in the same command.
- ❒ Adding a port to a group does not change its other group memberships because ports can belong to more than one group at a time. To move a port to a different group, you must remove it from its current group assignment before or after adding it to its new group.
- ❒ A group that does not have any upstream ports is placed in a suspended state. Downstream ports are permitted to forward traffic normally.
- ❒ A port stops forwarding network traffic if you add it as a downstream port to a group that does not have links on the upstream ports.

Examples

This command adds ports 5 and 6 as downstream ports of group 1:

```
add glc downstream 1 5,6
```

This command adds port 15 as an upstream port of group 2:

```
add glc downstream 2 15
```

AlliedWare Plus Command

Syntax

```
group link control upstream|downstream group
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Examples

This command adds port 12 as an upstream port to group 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 12
awplus(config-if)# group link control upstream 1
```

This command adds ports 12 to 15 as downstream ports to group 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 12-15
awplus(config-if)# group link control downstream 2
```

CREATE GLC

AlliedWare Plus
Command
Available

Syntax

```
create glc group [downstream_port] [upstream_port]
```

Parameters

group Specifies an ID number for a new group. The range is 1 to 8.

downstream_port Specifies a downstream port. You can specify more than one port.

upstream_port Specifies an upstream port. You can specify more than one port.

Description

This command is used to create new groups. Here are the guidelines:

- You can create groups with or without the ports. If you create a group without ports, you can add them later with the ADD GCL command, as explained in “ADD GLC” on page 428.
- This command does not activate group link control. That is performed separately with the standard ENABLE GLC command, as explained in “ENABLE GLC” on page 437.
- A new group is immediately functional if group link control is activated on the switch or stack. If there is no link on the upstream port, the downstream port will not forward traffic.

Examples

This command creates a new group with an ID number 1. Port 15 is a downstream port and port 2 is an upstream port.

```
create glc 1 15 2
```

This command creates a group with an ID number 2. No ports are specified. They will be added later with the ADD GLC command.

```
create glc 2
```

AlliedWare Plus Command

Syntax

```
group link control group
```

Mode

Configure mode

Description

There are several differences between this command and the standard command. First, this command automatically activates group link control when you create the first group. The standard commands have a separate command for activating the feature. Second, this command creates groups without any ports. You have to add the ports separately using the GROUP LINK CONTROL UPSTREAM|DOWNSTREAM command. For instructions, refer to the AlliedWare Plus command in “ADD GLC” on page 428.

Examples

This command creates a group with the ID number 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# group link control 1
```

This command creates a group with the ID number 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# group link control 3
```

DELETE GLC

AlliedWare Plus
Command
Available

Syntax

```
delete glc upstream|downstream group port
```

Parameters

upstream|downstream — Specifies whether a port is an upstream port or a downstream port of a group.

group — Specifies a group. You can specify only one group. The range is 1 to 8.

port — Specifies a port to remove from a group. You can specify more than one port.

Description

This command is used to remove ports from groups. Here are a few guidelines:

- You can remove either upstream ports or downstream ports, but not both in the same command.
- If you remove all of the upstream ports, a group is placed in a suspended state in which the downstream ports, if any, forward traffic normally.
- If you remove a downstream port that was disabled by group link control because there was no link on the upstream port, the removed port begins to forward traffic again.

Examples

This command removes upstream port 5 from group 1:

```
delete glc upstream 1 5
```

This command removes downstream ports 15 and 18 from group 2:

```
delete glc downstream 2 15,18
```

AlliedWare Plus Command

Syntax

```
no group link control upstream|downstream group
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Examples

This command removes upstream ports 15 and 17 from group 1:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15,17
awplus(config-if)# no group link control upstream 1
```

This command removes downstream port 11 from group 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11
awplus(config-if)# no group link control downstream 2
```

DESTROY GLC

AlliedWare Plus Command Available

Syntax

```
destroy glc group
```

Parameters

group	Specifies an ID number of a group to be deleted. You can delete only one group at a time. The range is 1 to 8.

Description

This command is used to delete groups from group link control. Here are a few guidelines:

- ❒ You do not have to delete the upstream and downstream ports before deleting a group.
- ❒ When a group is deleted, the downstream ports automatically resume forwarding traffic if they were disabled because there were no links on the upstream ports.
- ❒ If you delete the last group and want to disable group link control, refer to “DISABLE GLC” on page 436.

Examples

This command deletes group 1:

```
destroy glc 1
```

AlliedWare Plus Command

Syntax

```
no group link control group
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command. The only difference is this command disables group link control on the switch when you delete the last group.

Example

This example deletes group 2. If this is the last group on the switch, the command also disables group link control:

```
awplus> enable
awplus# configure terminal
awplus(config)# no group link control 2
```

DISABLE GLC

AlliedWare Plus
Command
Available

Syntax

```
disable glc
```

Parameters

None.

Description

This command is used to disable group link control on a switch or a stack. Here are a few guidelines:

- The defined groups remain, but the feature is disabled.
- The ports of the groups forward traffic normally, including any disabled downstream ports.

Example

This command disables group link control:

```
disable glc
```

AlliedWare Plus Command

The AlliedWare Plus NO GROUP LINK CONTROL command automatically disables the feature when you delete the last group on a switch or a stack. For instructions, refer to the AlliedWare Plus command in “DESTROY GLC” on page 434.

ENABLE GLC

AlliedWare Plus
Command
Available

Syntax

```
enable glc
```

Parameters

None.

Description

This command is used to enable group link control on a switch or a stack.

Example

This command enables group link control:

```
enable glc
```

AlliedWare Plus Command

The AlliedWare Plus GROUP LINK CONTROL command automatically activates the feature when you create the first group on a switch or a stack. For instructions, refer to the AlliedWare Plus command in "CREATE GLC" on page 430.

SHOW GLC

AlliedWare Plus
Command
Available

Syntax

```
show glc [group]
```

Parameters

group Specifies an ID number of a group to display. The range is 1 to 8. You can specify only one group. The command displays all of the groups if you omit this parameter.

Description

This command is used to display the groups for group link control on a switch or a stack. Figure 61 is an example of the information the command displays.

```
Group Link Control State .............. Enabled

ID .................................... 1
Status ................................ Up
Downstream (Link) Port(s) ............. 1.2
UPstream (Member) Port(s) ............. 1.3

ID .................................... 2
Status ................................ Up
Downstream (Link) Port(s) ............. 1.23
UPstream (Member) Port(s) ............. 1.24
```

Figure 61. SHOW GLC Command

The possible group status are:

- Up - The upstream and downstream ports are forwarding traffic because the upstream ports have links to network nodes.
- Down - Group link control has disabled the downstream ports to prevent them from forwarding traffic because the upstream ports do not have links to network nodes.
- Suspended - The group is incomplete, lacking either an upstream port or a downstream port. A downstream port in an incomplete group forwards traffic normally.

Examples

This command displays all of the groups on a switch or a stack:

```
show glc
```

This command displays just group 2:

```
show glc 2
```

AlliedWare Plus Command

Syntax

show group link control [*group*]

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This command displays all of the groups on a switch or a stack:

```
show group link control
```

This command displays just group 4:

```
show group link control 4
```

Chapter 23

Denial of Service Defense Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

SET DOS

Syntax

```
set dos ipaddress=ipaddress subnet=mask uplinkport=port
```

Parameters

ipaddress — Specifies the IP address of one of the devices connected to the switch, preferably the lowest IP address.

subnet — Specifies the subnet mask of the LAN. A binary “1” indicates the switch should filter on the corresponding bit of the address, while a “0” indicates that it should not.

uplinkport — Specifies the port on the switch that is connected to a device (for example, a DSL router) that leads outside the network. You can specify only one port. This parameter is required only for the Land defense. The default port is the highest numbered existing port in the switch.

Description

This command is required for the SMURF and Land defenses. The SMURF defense uses the LAN address and mask to determine the broadcast address of your network. The Land defense uses this information to determine which traffic is local and which is remote to your network.

As an example, assume that the devices connected to a switch are using the IP address range 149.11.11.1 to 149.11.11.50. The IP address would be 149.11.11.1 and the mask would be 0.0.0.63.

Examples

The following command sets the IP address to 149.11.11.1 and the mask to 0.0.0.63:

```
set dos ipaddress=149.11.11.1 subnet=0.0.0.63
```

The following command sets the IP address to 149.22.22.1, the mask to 0.0.0.255, and the uplink port for the Land defense to port 24:

```
set dos ipaddress=149.22.22.1 subnet=0.0.0.255 uplinkport=24
```

SET DOS IPOPTION

Syntax

```
set dos ipoption port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port Specifies the switch port where you want to enable or disable the IP Option defense. You can specify more than one port at a time.

state Specifies the state of the IP Option defense. The options are:

enable	Activates the defense.
disable	Deactivates the defense. This is the default.

mirroring Specifies whether the examined traffic is copied to a mirror port. Options are:

yes, on, true enabled	Traffic is mirrored. These values are equivalent.
no, off, false disabled	Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command enables and disables the IP Option DoS defense.

This type of attack occurs when an attacker sends packets containing bad IP options to a victim node. There are many different types of IP options attacks and the AT-S63 Management Software does not try to distinguish between them. Rather, a switch port where this defense is activated counts the number of ingress IP packets containing IP options. If the number exceeds 20 packets per second, the switch considers this a possible IP options attack and does the following occurs:

- The switch sends a trap to the management stations.
- The switch blocks all traffic on the port for one minute.

This defense mechanism does not involve the switch's CPU. You can activate it on as many ports as you want without it impacting switch performance.

You can use the MIRRORING parameter to copy the examined traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to “SET SWITCH MIRROR” on page 238.

Example

The following command activates the IP Options defense on ports 5, 7, and 10:

```
set dos ipoption port=5,7,10 state=enable
```

The following command activates the IP Options defense on port 6 as well as the mirroring feature so the examined traffic is copied to a destination port mirror.

```
set dos ipoption port=6 state=enable mirroring=yes
```

The following command disables the IP Options defense on ports 5 and 7:

```
set dos ipoption port=5,7 state=disable
```

SET DOS LAND

Syntax

```
set dos land port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port
: Specifies the switch port on which you want to enable or disable the Land defense. You can specify more than one port at a time.

state
: Specifies the state of the Land defense. The options are:

enable	Activates the defense.
disable	Deactivates the defense. This is the default.

mirroring
: Specifies whether the examined traffic is copied to a mirror port. Options are:

yes, on, true enabled	Traffic is mirrored. These values are equivalent.
no, off, false disabled	Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command enables and disables the Land DoS defense.

You can use the MIRRORING parameter to copy the intruding traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to "SET SWITCH MIRROR" on page 238.

Example

The following command activates the Land defense on ports 5 and 7:

```
set dos land port=5,7 state=enable
```

SET DOS PINGOFDEATH

Syntax

```
set dos pingofdeath port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port
: Specifies the switch ports on which to enable or disable the Ping of Death defense. You can specify more than one port at a time.

state
: Specifies the state of the IP Option defense. The options are:

enable	Activates the defense.
disable	Deactivates the defense. This is the default.

mirroring
: Specifies whether the examined traffic is copied to a mirror port. Options are:

yes, on, true enabled	Traffic is mirrored. These values are equivalent.
no, off, false disabled	Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command activates and deactivates the Ping of Death DoS defense.

In this DoS, an attacker sends an oversized, fragmented Ping packet to the victim, which, if lacking a policy for handling oversized packets, may freeze.

To defend against this form of attack, a switch port searches for the last fragment of a fragmented Ping request and examines its offset to determine if the packet size is greater than 63,488 bits. If it is, the fragment is forwarded to the switch’s CPU for final packet size determination. If the switch determines that the packet is oversized, the following occurs:

- The switch sends a trap to the management stations.
- The switch blocks all traffic on the port for one minute.

Note
This defense mechanism requires some involvement by the switch’s CPU, though not as much as the Teardrop defense. This will not impact the forwarding of traffic between the switch ports, but it can affect the handling of CPU events, like the processing of IGMP packets and spanning tree BPDUs. For this reason, Allied Telesis recommends limiting the use of this defense to only those ports where an attack is likely to originate.

You can use the MIRRORING parameter to copy the offending traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to “SET SWITCH MIRROR” on page 238.

Example

The following command activates the defense on ports 1 and 5:

```
set dos pingofdeath port=1,5 state=enable
```

SET DOS SMURF

Syntax

```
set dos smurf port=port state=enable|disable
```

Parameters

port	Specifies the switch ports on which you want to enable or disable SMURF defense. You can select more than one port at a time.	
state	Specifies the state of the SMURF defense. The options are:	
	enable	Activates the defense.
	disable	Deactivates the defense. This is the default.

Description

This command activates and deactivates the SMURF DoS defense.

This DoS attack is instigated by an attacker sending a Ping request containing a broadcast address as the destination address and the address of the victim as the source of the Ping. This overwhelms the victim with a large number of Ping replies from other network nodes.

A switch port defends against this form of attack by examining the destination addresses of ingress Ping packets and discarding those that contain a broadcast address as a destination address.

To implement this defense, you need to specify the IP address of any device on your network, preferably the lowest IP address, and a mask using “SET DOS” on page 442. The switch uses the combination of the two to determine your network’s broadcast address. Any ingress Ping packets containing the broadcast address are discarded.

This defense mechanism does not involve the switch’s CPU. You can activate it on as many ports as you want without having it negatively impact switch performance.

Example

The following command activates this defense on port 17:

```
set dos smurf port=17 state=enable
```

SET DOS SYNFLOOD

Syntax

```
set dos synflood port=port state=enable|disable
```

Parameters

port — Specifies the switch ports on which you want to enable or disable this DoS defense. You can select more than one port at a time.

state — Specifies the state of the DoS defense. The options are:

enable	Activates the defense.
disable	Deactivates the defense. This is the default.

Description

This command activates and deactivates the SYN ACK Flood DoS defense.

In this type of attack, an attacker, seeking to overwhelm a victim with TCP connection requests, sends a large number of TCP SYN packets with bogus source addresses to the victim. The victim responds with SYN ACK packets, but since the original source addresses are bogus, the victim node does not receive any replies. If the attacker sends enough requests in a short enough period, the victim may freeze operations once the requests exceed the capacity of its connections queue.

To defend against this form of attack, a switch port monitors the number of ingress TCP-SYN packets it receives. If a port receives more 60 TCP-SYN packets per second, the following occurs.

- The switch sends a trap to the management stations
- The switch blocks all traffic on the port for one minute.

This defense mechanism does not involve the switch's CPU. You can activate it on as many ports as you want without it impacting switch performance.

Example

The following command activates the defense on ports 18 to 20:

```
set dos synflood port=18-20 state=enable
```

SET DOS TEARDROP

Syntax

```
set dos teardrop port=port state=enable|disable
[mirroring=yes|no|on|off|true|false|enabled|disabled]
```

Parameters

port	Specifies the switch ports on which you want to enable or disable this DoS defense. You can select more than one port at a time.	
state	Specifies the state of the DoS defense. The options are:	
	enable	Activates the defense.
	disable	Deactivates the defense. This is the default.
mirroring	Specifies whether the examined traffic is copied to a mirror port. Options are:	
	yes, on, true enabled	Traffic is mirrored. These values are equivalent.
	no, off, false disabled	Traffic is not mirrored. This is the default. These values are equivalent.

Description

This command activates and deactivates the Teardrop DoS defense.

In this DoS attack, an attacker sends a packet in several fragments with a bogus offset value, used to reconstruct the packet, in one of the fragments to a victim. This results in the victim being unable to reassemble the packet, possibly causing it to freeze operations.

The defense mechanism for this type of attack has all ingress IP traffic received on a port sent to the switch’s CPU. The CPU samples related, consecutive fragments, checking for fragments with invalid offset values. If one is found, the following occurs:

- ❒ The switch sends a trap to the management stations.
- ❒ The switch blocks all traffic on the port for one minute.

Because the CPU examines only a sampling of the ingress IP traffic on a port, there is no guarantee that the switch will catch or prevent all occurrences of this attack.

You can use the MIRRORING parameter to copy the offending traffic to a destination port mirror for analysis with a data analyzer. To define the destination port, refer to “SET SWITCH MIRROR” on page 238.

Caution

This defense is extremely CPU intensive and should be used with caution. Unrestricted use can cause a switch to halt operations if the CPU becomes overwhelmed with IP traffic. To prevent this, Allied Telesis recommends that you activate this defense on only one port at a time and where ingress fragments comprise only a small percentage of the port's total traffic.

Example

The following command activates the defense on port 22:

```
set dos teardrop port=22 state=enable
```

SHOW DOS

Syntax 1

```
show dos [ipaddress] [subnet] [uplinkport]
```

Syntax 2

```
show dos defense port=port
```

Parameters

ipaddress Displays the IP address of the LAN.

subnet Displays the subnet mask.

uplinkport Displays the uplink port for the Land defense.

defense Displays the status of a specified defense for a particular port. Defense can be any of the following:

synflood

smurf

land

teardrop

ipoption

pingofdeath

port Specifies the port whose DoS status you want to view. You can specify only one port.

Description

These commands display DoS status information. Syntax 1 displays the current settings for the IP address, subnet mask, and uplink port parameters. Syntax 2 displays DoS status information for a specific defense mechanism on a specific port.

Examples

The following command displays the IP address and subnet mask for the Land and SMURF defenses:

```
show dos ipaddress subnet
```

The following command displays the status of the SMURF defense on port 4:

```
show dos smurf port=4
```

Chapter 24

Power Over Ethernet Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	
AT-9424T/POE	Yes
AT-9424Ts	
AT-9424Ts/XP	
AT-9448T/SP	
AT-9448Ts/XP	
AT-9400Ts Stack	

This chapter contains the following commands:

- “DISABLE POE PORT” on page 456
- “ENABLE POE PORT” on page 457
- “SET POE PORT” on page 458
- “SET POE POWERTHRESHOLD” on page 460
- “SHOW POE CONFIG” on page 461
- “SHOW POE STATUS” on page 462

DISABLE POE PORT

Syntax

```
disable poe port=port
```

Parameters

port	Specifies a port. You can configure more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

Description

This command disables PoE on a port. The default setting for PoE on a port is enabled. Ports provide standard Ethernet connectivity even when PoE is disabled.

Examples

This command disables PoE on ports 5 and 7:

```
disable poe port=5,7
```

ENABLE POE PORT

Syntax

```
enable poe port=port
```

Parameters

port	Specifies a port. You can configure more than one port at a time. For instructions on how to enter port numbers, refer to "Port Numbers in Commands" on page 48.

Description

This command activates PoE on the ports. The default setting for PoE is enabled.

Examples

This commands activates PoE on port 2:

```
enable poe port=2
```

SET POE PORT

Syntax

```
set poe port=port [poefunction=enable|disable]
[priority=low|high|critical] [powerlimit=value]
```

Parameters

port	Specifies a port. You can configure more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.
poefunction	Enables and disables PoE on a port. The default setting is enabled. This parameter is equivalent to the DISABLE POE PORT and DISABLE POE PORT commands.
priority	Specifies the port’s priority as LOW, HIGH, or CRITICAL.
powerlimit	Specifies the maximum amount of power the powered device is allowed to draw from the port. The value is specified in milliwatts (mW). The range is 3,000 to 15,400 mW. The default value is the maximum amount 15,400 mW.

Description

This command configures the PoE settings on a port.

The POEFUNCTION parameter enables and disables PoE on the ports. The default setting is enabled. This parameter is equivalent to the DISABLE POE PORT and DISABLE POE PORT commands.

The PRIORITY parameter is used to set the priorities of the ports. If the power requirements of the devices exceed the power resources of a switch, power is supplied or denied to the ports based on their port priorities. You can use this parameter to ensure that powered devices critical to the operations of your network are given preferential treatment by the switch in the distribution of power should the demands of the devices exceed the available capacity.

There are three priority levels:

- Critical
- High
- Low

The Critical level is the highest priority level. Ports set to this level are guaranteed power before any ports assigned to the other two priority levels. Ports assigned to the other priority levels receive power only if all the Critical ports are receiving power. Your most critical powered devices should be assigned to this level. If there is not enough power to support all the ports set to the Critical priority level, power distribution is based on port number, in ascending order.

The High level is the second highest level. Ports set to this level receive power only if all the ports set to the Critical level are already receiving power. If there is not enough power to support all of the ports set to the High priority level, power is provided to the ports based on port number, in ascending order.

The lowest priority level is Low. This is the default setting. Ports set to this level only receive power if all the ports assigned to the other two levels are already receiving power. As with the other levels, if there is not enough power to support all of the ports set to the Low priority level, power is provided to the ports based on port number, in ascending order.

Power allocation is dynamic. Ports supplying power to powered devices may cease power transmission if the switch’s power budget has reached maximum usage and new powered devices, connected to ports with a higher priority, become active.

The POWERLIMIT parameter in this command sets the maximum amount of power a powered device can draw from the port. The value is set in milliwatts. The default is 15400 mW (15.4 W).

Examples

This command disables PoE on ports 4 and 5:

```
set poe port=4-5 poefunction=disable
```

This command sets the priority on ports 6 and 11 to high:

```
set poe port=6,11 priority=high
```

This commands sets the maximum power on port 14 to 12,500 mW:

```
set poe port=14 powerlimit=12500
```

SET POE POWERTHRESHOLD

Syntax

```
set poe powerthreshold=value
```

Parameters

threshold Specifies the threshold as a percentage of the total amount of PoE available. The range is 1 to 100.

Description

This command lets you specify a power threshold for the powered devices that are connected to the switch. If the total power requirements of the devices exceed the threshold, the switch enters an event in the event log and sends an SNMP trap to your management workstation. The threshold is entered as a percentage of the total amount of power on the switch for the powered devices. At the default setting of 95%, the threshold is 361 W, which is 95% of 380 W, the maximum power on the AT-9424T/POE Switch for the powered devices.

Examples

This command sets the threshold to 80% of the available power:

```
set poe threshold=80
```

SHOW POE CONFIG

Syntax

```
show poe config [port=port]
```

Parameter

port — Specifies a port. You can view more than one port at a time. For instructions on how to enter port numbers, refer to "Port Numbers in Commands" on page 48.

Description

Entering this command without specifying a port displays the following PoE information:

- ❒ Maximum available power - The total amount of available power on the switch for powered devices. This value is 380 W for the AT-9424T/POE switch.
- ❒ Power threshold - The percentage of the maximum available power which, if exceeded by the powered devices, causes the switch to send an SNMP trap to your management workstation and enter an event in the event log. At the default setting of 95%, the switch sends an SNMP trap when the PoE devices require more than 361 W, which is 95% of 380 W, the maximum available power on the AT-9424T/POE switch.

Entering the command with the PORT parameter, displays this PoE information about the specified port:

- ❒ PoE function - The status of PoE on a port, which can be either enabled or disabled. The default is enabled.
- ❒ Power priority - The port's priority, which can be critical, high, or low. The default is low.
- ❒ Power limit - The maximum amount of power available to a powered device. The default value is 15.4 W.

Examples

This command displays general PoE information:

```
show poe config
```

This command displays PoE information for port 4:

```
show poe config port=4
```

SHOW POE STATUS

Syntax

```
show poe status [port=port]
```

Parameter

port	Specifies a port. You can view more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

Description

Entering this command without specifying a port displays the following PoE information:

- ❒ Max Available Power - The total available power for PoE supplied by the switch. This value is 380 W for the AT-9424T/POE switch.
- ❒ Consumed Power - The amount of power being used by the powered devices.
- ❒ Available Power - The amount of power available for additional powered devices.
- ❒ Power Usage - The amount of power currently consumed by the powered devices connected to the switch. The value is give as a percentage of the total amount of power available.
- ❒ Min Shutdown Voltage - The minimum threshold voltage at which the switch shuts down PoE. If the power supply in the switch experiences a problem and the output voltage drops below this value, the switch shuts down PoE on all ports. This value is not adjustable.
- ❒ Max Shutdown Voltage - The maximum threshold voltage at which the switch shuts down PoE. If the power supply in the switch experiences a problem and the output voltage exceeds this value, the switch shuts down PoE on all ports. This value is not adjustable.
- ❒ Summary of port status

Specifying a port in the command displays the following PoE information about the port:

- ❒ PoE Function - Whether PoE is enabled or disabled on the port. The default setting is enabled. To enable or disable PoE on a port, refer to “ENABLE POE PORT” on page 457 and “DISABLE POE PORT” on page 456.
- ❒ Power Status - Whether power is being supplied to the device. ON means that the port is providing power to a powered device. OFF means the device is not a powered device or PoE has been disabled on the port.

- Power Consumed - The amount of power in milliwatts currently consumed by the powered device connected to the port. If the port is not connected to a powered device, this value will be 0 (zero).
- Power Limit - The maximum amount of power allowed by the port for the device. The default is 15,400 milliwatts (15.4 W). To adjust this value for a port, refer to “SET POE PORT” on page 458.
- Power Priority - The port priority. This can be Critical, High, or Low. To adjust this value, refer to “SET POE PORT” on page 458.
- Power Class - The IEEE 802.3af class of the device.
- Voltage - The voltage being provided to the powered device
- Current - The current drawn by the powered device.

Examples

This command displays general PoE information:

```
show poe status
```

This command displays PoE information for port 4:

```
show poe status port=4
```

Section III

Snooping Protocols

This section has the following chapters:

Chapter 25

Internet Group Management Protocol (IGMP) Snooping Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

DISABLE IGMPSNOOPING

AlliedWare Plus Command Available

Syntax

```
disable igmpsnooping
```

Parameters

None.

Description

This command deactivates IGMP snooping on the switch. This command also removes IGMP querier from its VLAN assignments.

Example

The following command deactivates IGMP snooping:

```
disable igmpsnooping
```

Equivalent Command

```
set ip igmp snoopingstatus=disabled
```

For information, refer to “SET IP IGMP” on page 470.

AlliedWare Plus Command

Syntax

```
no ip igmp snooping
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp snooping
```

ENABLE IGMPSNOOPING

AlliedWare Plus
Command
Available

Syntax

```
enable igmpsnooping
```

Parameters

None.

Description

This command activates IGMP snooping on the switch.

Example

The following command activates IGMP snooping:

```
enable igmpsnooping
```

Equivalent Command

```
set ip igmp snoopingstatus=enabled
```

For information, refer to “SET IP IGMP” on page 470.

AlliedWare Plus Command

Syntax

```
ip igmp snooping
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp snooping
```

SET IP IGMP

AlliedWare Plus
Command
Available

Syntax

```
set ip igmp [snoopingstatus=enabled|disabled]
[hoststatus=singlehost|multihost] [timeout=value]
[numbermulticastgroups=value]
[routerport=port|all|none|auto]
```

Parameters

snoopingstatus

Activates and deactivates IGMP snooping on the switch. The options are:

- enabled: Activates IGMP snooping.
- disabled: Deactivates IGMP snooping. This is the default setting.

hoststatus

Specifies the IGMP host node topology. Options are:

- singlehost: Activates the Single-Host/Port setting, which is appropriate when there is only one host node connected to a port on the switch. This is the default setting.
- multihost: Activates the Multi-Host setting, which is appropriate if there is more than one host node connected to a switch port.

timeout

Specifies the time period in seconds used to identify inactive host nodes. Inactive host nodes are nodes that do not sent IGMP reports during the specified time interval. The range is from 0 second to 86,400 seconds (24 hours). The default is 260 seconds. Setting the timeout to zero (0) disables the timer.

This parameter also controls the time interval used by the switch to determine whether a multicast router is still active. The switch makes the determination by watching for queries from the router. If the switch does not detect any queries from a multicast router during the specified time interval, the router is assumed to be no longer active on the port.

The actual timeout may be ten seconds less that the specified value. For example, a setting of 25 seconds can result in the switch classifying a host node or multicast router as inactive after just 15 seconds. A setting of 10 seconds or less can result in the immediate timeout of an inactive host node or router.

numbermulticastgroups

Specifies the maximum number of multicast addresses the switch can learn. This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 0 to 255 addresses; the default is 64 addresses.

Note
The combined maximum number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

routerport

Specifies the port(s) on the switch connected to a multicast router. Options are:

port — Specifies the router port(s) manually.

all — Specifies all the switch ports.

none — Sets the mode to manual without any router ports specified.

auto — Activates auto-detect, where the switch automatically determines the ports with multicast routers.

Description

This command is used to configure the IGMP snooping parameters.

Examples

The following command activates IGMP snooping, sets the IGMP topology to Multi-Host, and sets the timeout value to 120 seconds:

```
set ip igmp snoopingstatus=enabled hoststatus=multihost
timeout=120
```

The following command changes the topology to Single-Host:

```
set ip igmp hoststatus=singlehost
```

The following command disables IGMP snooping:

```
set ip igmp snoopingstatus=disabled
```

Equivalent Commands

```
disable igmpsnooping
```

For information, refer to “DISABLE IGMPSNOOPING” on page 468.

```
enable igmpsnooping
```

For information, refer to “ENABLE IGMPSNOOPING” on page 469.

AlliedWare Plus Command

Syntax

To set the maximum number of multicast addresses the switch can learn:

```
ip igmp limit numbermulticastgroups
```

To set the time-out period for inactive host nodes:

```
ip igmp querier-timeout timeout
```

To set the host node topology:

```
ip igmp status single|multiple
```

To specify a router port:

```
ip igmp router interface port
```

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example sets the maximum number of multicast groups to 25:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp limit 25
```

This example sets the timeout for inactive nodes to 400 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp querier-timeout 400
```

This example sets the host node topology to multiple nodes:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp status multiple
```

This example sets the router port to port 14:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp router interface 14
```

SHOW IGMPSNOOPING

AlliedWare Plus
Command
Available

Syntax

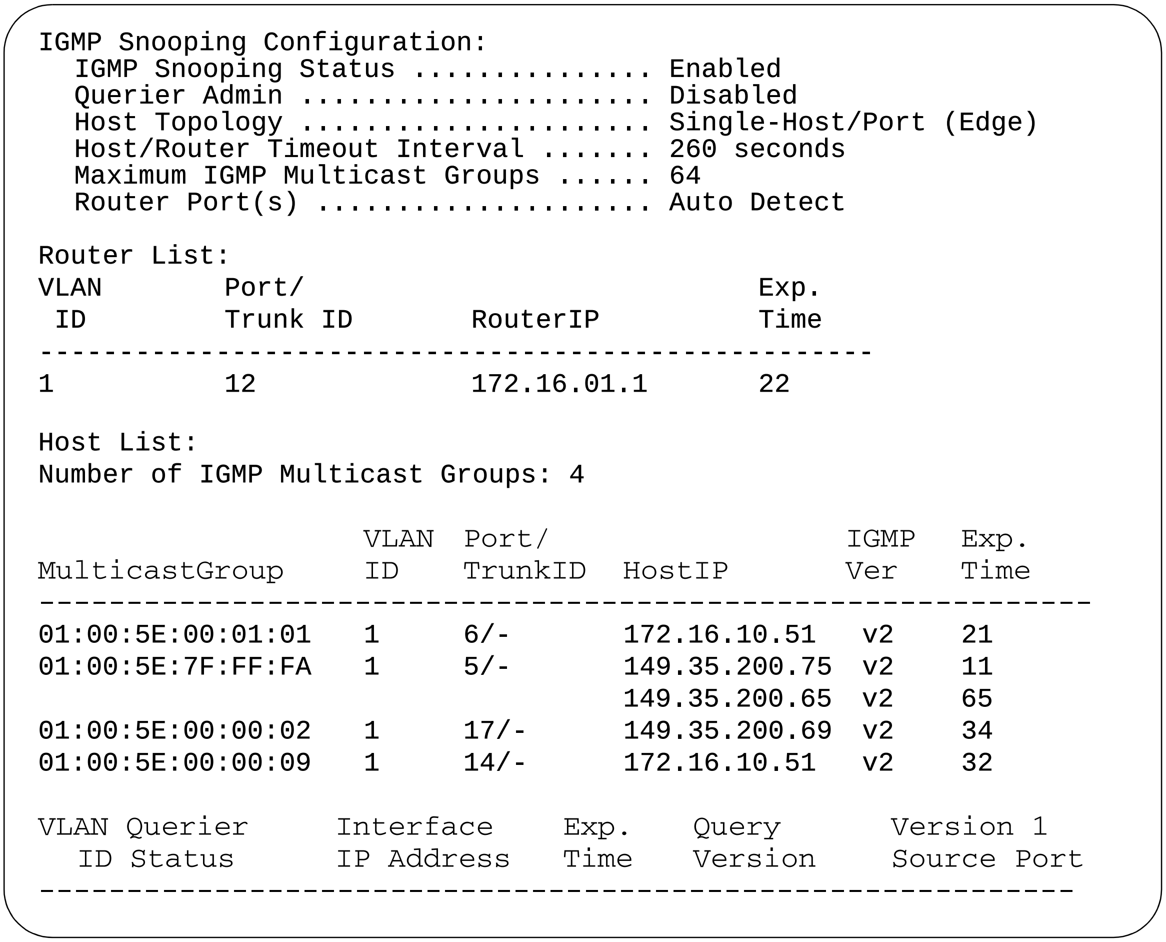
```
show igmpsnooping
```

Parameters

None.

Description

This command displays the IGMP parameters. Figure 62 illustrates the information.



```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Enabled
  Querier Admin ...................... Disabled
  Host Topology ...................... Single-Host/Port (Edge)
  Host/Router Timeout Interval ....... 260 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect

Router List:
VLAN       Port/                       Exp.
 ID        Trunk ID       RouterIP         Time
----------------------------------------------------
1          12             172.16.01.1      22

Host List:
Number of IGMP Multicast Groups: 4

                    VLAN  Port/                  IGMP   Exp.
MulticastGroup      ID    TrunkID  HostIP        Ver    Time
-----------------------------------------------------------------
01:00:5E:00:01:01   1     6/-      172.16.10.51   v2    21
01:00:5E:7F:FF:FA   1     5/-      149.35.200.75  v2    11
                                   149.35.200.65  v2    65
01:00:5E:00:00:02   1     17/-     149.35.200.69  v2    34
01:00:5E:00:00:09   1     14/-     172.16.10.51   v2    32

VLAN Querier      Interface    Exp.    Query       Version 1
  ID Status       IP Address   Time    Version     Source Port
----------------------------------------------------------------
```

Figure 62. SHOW IGMPSNOOPING Command

For an explanation of these parameters, refer to “SET IP IGMP” on page 470 and “SHOW IP IGMP” on page 476.

Example

The following command displays the current IGMP parameter settings:

```
show igmpsnooping
```

Equivalent Command

```
show ip igmp
```

For information, see “SHOW IP IGMP” on page 476.

```
show ip igmp querierlist
```

For information, see “SHOW IP IGMP QUERIERLIST” on page 482.

AlliedWare Plus Command

Syntax

```
show ip igmp snooping
```

Mode

User Exec mode and Privileged Exec mode

Description

This command is equivalent to the standard command.

Example

```
awplus# show ip igmp snooping
```

SHOW IP IGMP

Syntax

```
show ip igmp [hostlist] [routerlist]
```

Parameters

hostlist	Displays a list of the multicast groups learned by the switch, as well as the ports on the switch that are connected to host nodes. This parameter displays information only when there are active host nodes.
routerlist	Displays the ports on the switch where multicast routers are detected. This parameter displays information only when there are active multicast routers.

Description

This command displays the IGMP parameters. Figure 63 illustrates the information that is displayed by this command without the optional parameters.

```
IGMP Snooping Configuration:
  IGMP Snooping Status ............... Enabled
  Querier Admin ...................... Disabled
  Host Topology ...................... Single-Host/Port (Edge)
  Host/Router Timeout Interval ....... 260 seconds
  Maximum IGMP Multicast Groups ...... 64
  Router Port(s) ..................... Auto Detect
```

Figure 63. SHOW IP IGMP Command

For an explanation of these parameters, refer to “SET IP IGMP” on page 470.

An example of the information displayed by the HOSTLIST parameter is shown in Figure 64.

```
Number of IGMP Multicast Groups: 4

                    VLAN  Port/                        IGMP   Exp.
MulticastGroup      ID    TrunkID   HostIP             Ver    Time
-------------------------------------------------------------------
01:00:5E:00:01:01   1     6/-       172.16.10.51   v2     21
01:00:5E:7F:FF:FA   1     5/-       149.35.200.75  v2     11
                                    149.35.200.65  v2     65
01:00:5E:00:00:02   1     17/-      149.35.200.69  v2     34
01:00:5E:00:00:09   1     14/-      172.16.10.51   v2     32
```

Figure 64. SHOW IP IGMP Command with HOSTLIST Parameter

The HOSTLIST parameter displays the following information:

- Number of IGMP Multicast Groups - The number of IGMP multicast groups with active host nodes on the switch.
- Multicast Group - The multicast address of the group.
- VLAN - The VID of the VLAN where the port or trunk is an untagged member.
- Port/Trunk - The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number instead of the port number is displayed.
- HostIP - The IP address of the host node connected to the port.
- IGMP Ver. - The version of IGMP being used by the host.
- Exp. Time - The number of seconds remaining before the host is timed out if no further IGMP reports are received from it.

An example of the information displayed by the ROUTERLIST parameter is shown in Figure 65.

```
Router List:
VLAN        Port/                          Exp.
 ID         Trunk ID       RouterIP        Time
----------------------------------------------------
1           12             172.16.01.1     22
```

Figure 65. SHOW IP IGMP Command with ROUTERLIST Parameter

The ROUTERLIST parameter displays the following information:

- VLAN - The VID of the VLAN in which the port is an untagged member.
- Port/Trunk ID - The port on the switch where the multicast router is connected. If the switch learned the router on a port trunk, the trunk ID number instead of the port number is displayed.

❒ Router IP - The IP address of the multicast router.

Examples

The following command displays the current IGMP parameter settings:

```
show ip igmp
```

The following command displays a list of active host nodes connected to the switch:

```
show ip igmp hostlist
```

The following command displays a list of active multicast routers:

```
show ip igmp routerlist
```

Equivalent Command

```
show igmpsnooping
```

This command does not display the router and host lists. For information, see “SHOW IGMPSNOOPING” on page 474.

Chapter 26

Internet Group Management Protocol (IGMP) Snooping Querier Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

SET IP IGMP QUERIER

AlliedWare Plus Command Available

Syntax

```
set ip igmp querier enable|disable vlan=vid
```

Parameters

vlan	Specifies the ID of the VLAN where you want to add or remove IGMP querier.

Description

This command is used to add and remove IGMP snooping querier from a VLAN. The ENABLE option adds it to a VLAN and the DISABLE option removes it. If you are adding IGMP snooping querier to a VLAN, follow these guidelines:

- ❒ IGMP snooping must be enabled on the switch.
- ❒ The VLAN must already exist.
- ❒ The VLAN must have a routing interface.
- ❒ The IP address of the interface must be a member of the same subnet as the multicast source.

Examples

This command adds IGMP snooping querier to a VLAN with the ID 2:

```
set ip igmp querier enable vlan=2
```

This command removes IGMP snooping querier from a VLAN with the ID 2:

```
set ip igmp querier disable vlan=2
```

AlliedWare Plus Command

Syntax

To add IGMP querier to a VLAN:

```
ip igmp querier-list vid
```

To remove IGMP querier from a VLAN:

```
no ip igmp querier vid
```

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example adds IGMP querier to a VLAN with the ID 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip igmp querier-list 2
```

This example removes IGMP querier from a VLAN with the ID 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip igmp querier 2
```

SHOW IP IGMP QUERIERLIST

AlliedWare Plus
Command
Available

Syntax

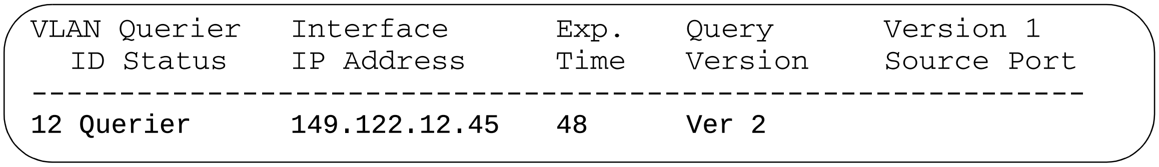
```
show ip igmp querierlist
```

Parameters

None.

Description

This command displays the IGMP snooping querier parameters. Figure 66 illustrates the information.



```
VLAN Querier   Interface       Exp.    Query        Version 1
  ID Status    IP Address      Time    Version      Source Port
------------------------------------------------------------------
12 Querier     149.122.12.45   48      Ver 2
```

Figure 66. SHOW IP IGMP QUERIER Command

The columns are defined here:

- VLAN Querier ID Status: This column displays the ID of the VLAN where IGMP snooping querier is added.
- Interface IP Address: This column displays the IP address of the routing interface in the VLAN.
- Exp. Time: The amount of time remaining before the switch sends another query. When the querier is first enabled, the switch sends a query every 31 seconds three times. Afterwards, it sends queries every 125 seconds.
- Query Version: The type of queries the switch is sending. This will be either version 1 or 2.
- Version 1 Source Ports: If there are nodes that are sending version 1 requests, this column lists their port numbers.

AlliedWare Plus Command

Syntax

```
show ip igmp querier
```

Mode

User Exec mode and Privileged Exec mode

Description

This command is equivalent to the standard command.

Example

```
show ip igmp querier
```

Chapter 27

Multicast Listener Discovery (MLD) Snooping Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

- “DISABLE MLDSNOOPING” on page 486
- “ENABLE MLDSNOOPING” on page 487
- “SET IPV6 MLDSNOOPING” on page 488
- “SHOW MLDSNOOPING” on page 492
- “SHOW IPV6 MLDSNOOPING” on page 495

DISABLE MLDSNOOPING

AlliedWare Plus
Command
Available

Syntax

```
disable mldsnooping
```

Parameters

None.

Description

This command deactivates MLD snooping on the switch.

Example

The following command deactivates MLD snooping:

```
disable mldsnooping
```

Equivalent Command

```
set ipv6 mldsnooping snoopingstatus=disabled
```

For information, refer to “SET IPV6 MLDSNOOPING” on page 488.

AlliedWare Plus Command

Syntax

```
no ip mld snooping
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip mld snooping
```

ENABLE MLDSNOOPING

AlliedWare Plus Command Available

Syntax

```
enable mldsnooping
```

Parameters

None.

Description

This command activates MLD snooping on the switch.

Example

The following command activates MLD snooping:

```
enable mldsnooping
```

Equivalent Command

```
set ipv6 mldsnooping snoopingstatus=enabled
```

For information, refer to "SET IPV6 MLDSNOOPING" on page 488.

AlliedWare Plus Command

Syntax

```
ip mld snooping
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# ip mld snooping
```

SET IPV6 MLDSNOOPING

AlliedWare Plus
Command
Available

Syntax

```
set ipv6 mldsnooping [snoopingstatus=enabled|disabled]
[hoststatus=singlehost|multihost] [timeout=value]
[numbermulticastgroups=value]
[routerport=port|all|none|auto]
```

Parameters

snoopingstatus

Activates and deactivates MLD snooping on the switch. The options are:

enabled — Activates MLD snooping.

disabled — Deactivates MLD snooping. This is the default setting.

hoststatus

Specifies the MLD host node topology. Options are:

singlehost — Activates the Single-Host/Port setting, which is appropriate when there is only one host node connected to a port on the switch. This is the default setting.

multihost — Activates the Multi-Host setting, which is appropriate if there is more than one host node connected to a switch port.

timeout

Specifies the time period, in seconds, used by the switch in determining inactive host nodes. An inactive host node is a node that has not sent an MLD report during the specified time interval. The range is 1 to 86,400 seconds (24 hours); the default is 260 seconds.

numbermulticastgroups

Specifies the maximum number of multicast addresses the switch learns. This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 to 255 addresses; the default is 64 addresses.

Note
The combined number of multicast address groups for IGMP and MLD snooping cannot exceed 255.

routerport — Specifies the port(s) on the switch connected to a multicast router. Options are:

port — Specifies the router port(s) manually.

all — Specifies all of the switch ports.

none — Sets the mode to manual without any router ports specified.

auto — Activates auto-detect, where the switch automatically determines the ports with multicast routers.

Description

This command configures the MLD snooping parameters.

Examples

The following command activates MLD snooping, sets the MLD topology to Multi-Host, and sets the timeout value to 120 seconds:

```
set ipv6 mldsnooping snoopingstatus=enabled
hoststatus=multihost timeout=120
```

The following command changes the topology to Single-Host:

```
set ipv6 mldsnooping hoststatus=singlehost
```

The following command disables MLD snooping:

```
set ipv6 mldsnooping snoopingstatus=disabled
```

Equivalent Commands

```
disable mldsnooping
```

For information, see “DISABLE MLDSNOOPING” on page 486.

```
enable mldsnooping
```

For information, see “ENABLE MLDSNOOPING” on page 487.

AlliedWare Plus Command

Syntax

To enable MLD snooping:

```
ip mld snooping
```

To disable MLD snooping:

```
no ip mld snooping
```

To set the host node topology:

```
ip mld status single|multiple
```

To set the time-out period for inactive host nodes:

```
ip mld querier-timeout timeout
```

To set the maximum number of multicast addresses the switch can learn:

```
ip mld limit numbermulticastgroups
```

To specify a router port:

```
ip mld router interface port
```

Mode

Configure mode

Description

The only difference between these AlliedWare Plus commands and the standard command is you can specify only one router port with the IP MLD ROUTER INTERFACE command. To specify more than one port or to activate auto-detect, use the standard command.

Examples

This example sets the host node topology to multiple nodes:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip mld status multiple
```

This example sets the timeout for inactive nodes to 400 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip mld querier-timeout 400
```

This example sets the maximum number of multicast groups to 25:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip mld limit 25
```

This example sets the router port to port 14:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip mld router interface 14
```

SHOW MLDSNOOPING

AlliedWare Plus Command Available

Syntax

```
show mldsnooping
```

Parameters

None.

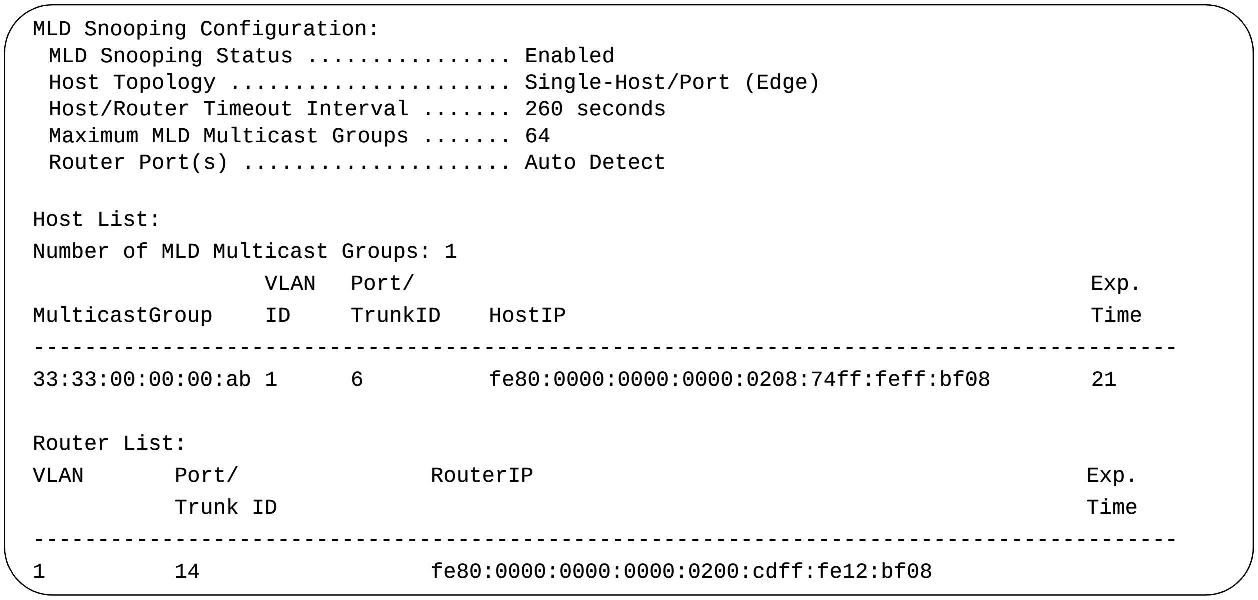
Description

This command displays the following MLD parameters:

- MLD snooping status
- Multicast host topology
- Host/router timeout interval
- Maximum multicast groups
- Host and router lists

To set the MLD parameters, refer to “SET IPV6 MLDSNOOPING” on page 488.

This command displays the information in Figure 67.



```
MLD Snooping Configuration:
 MLD Snooping Status ................ Enabled
 Host Topology ...................... Single-Host/Port (Edge)
 Host/Router Timeout Interval ....... 260 seconds
 Maximum MLD Multicast Groups ....... 64
 Router Port(s) ..................... Auto Detect

Host List:
Number of MLD Multicast Groups: 1
                  VLAN   Port/                                                Exp.
MulticastGroup    ID     TrunkID    HostIP                                    Time
-----------------------------------------------------------------------------------------
33:33:00:00:00:ab 1      6          fe80:0000:0000:0000:0208:74ff:feff:bf08       21

Router List:
VLAN       Port/              RouterIP                                        Exp.
           Trunk ID                                                           Time
-----------------------------------------------------------------------------------------
1          14                 fe80:0000:0000:0000:0200:cdff:fe12:bf08
```

Figure 67. SHOW MLDSNOOPING Command

The parameters in the MLD Snooping Configuration section are explained “SET IPV6 MLDSNOOPING” on page 488.

The Host List section displays the following information:

- Multicast Group - The multicast address of the group.
- VLAN - The VID of the VLAN where the port is an untagged member.
- Port/TrunkID - The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number, not the port number, is displayed.
- HostIP - The IP address of the host node connected to the port.
- Exp. Time - The number of seconds remaining before the host is timed out if no further MLD reports are received from it.

The Router List section displays this information:

- VLAN - The VID of the VLAN in which the port is an untagged member.
- Port/Trunk ID - The port on the switch where the multicast router is connected. If the switch learned the router on a port trunk, the trunk ID number, not the port number, is displayed.
- Router IP - The IP address of the multicast router.

Example

The following command displays the current MLD parameter settings, along with the host and router lists:

```
show mldsnooping
```

Equivalent Command

```
show ipv6 mldsnooping hostlist routerlist
```

For information, see “SHOW IPV6 MLDSNOOPING” on page 495.

AlliedWare Plus Command

Syntax

```
show ip mld snooping
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show ip mld snooping
```

SHOW IPV6 MLDSNOOPING

Syntax

```
show ipv6 mldsnooping [hostlist] [routerlist]
```

Parameters

hostlist — Displays a list of the multicast groups learned by the switch, as well as the ports on the switch that are connected to host nodes. This parameter displays information only when there are active host nodes.

routerlist — Displays the ports on the switch where multicast routers are detected. This parameter displays information only when there are active multicast routers.

Description

This command displays the following MLD parameters:

❒ MLD snooping status

❒ Multicast host topology

❒ Host/router timeout interval

❒ Maximum multicast groups

❒ Multicast router port(s)

❒ Host and router lists

For instructions on how to set the MLD parameters, refer to “SET IPV6 MLDSNOOPING” on page 488.

This command without optional parameters displays the information in Figure 68.

```
MLD Snooping Configuration:
 MLD Snooping Status ................ Enabled
 Host Topology ...................... Single-Host/Port (Edge)
 Host/Router Timeout Interval ....... 260 seconds
 Maximum MLD Multicast Groups ....... 64
 Router Port(s) ..................... Auto Detect
```

Figure 68. SHOW IPV6 MLDSNOOPING Command

Refer to “SET IPV6 MLDSNOOPING” on page 488 for an explanation of the parameters.

The HOSTLIST option displays the information in Figure 69.

```
Host List:
Number of MLD Multicast Groups: 1
                        VLAN    Port/                                               Exp.
MulticastGroup          ID      TrunkID    HostIP                                   Time
--------------------------------------------------------------------------------------------
33:33:00:00:00:ab       1       6          fe80:0000:0000:0000:0208:74ff:feff:bf08      21
```

Figure 69. SHOW IPV6 MLDSNOOPING Command with HOSTLIST Option

The information is described here:

- Multicast Group - The multicast address of the group.
- VLAN - The VID of the VLAN where the port is an untagged member.
- Port/TrunkID - The port on the switch where the host node is connected. If the host node is connected to the switch through a trunk, the trunk ID number, not the port number, is displayed.
- HostIP - The IP address of the host node connected to the port.
- Exp. Time - The number of seconds remaining before the host is timed out if no further MLD reports are received from it.

The ROUTERLIST option displays the information in Figure 70.

```
Router List:
VLAN   Port/Trunk ID   RouterIP
--------------------------------------------------------------
1      14              fe80:0000:0000:0000:0200:cdff:fe12:bf08
```

Figure 70. SHOW IPV6 MLDSNOOPING Command with ROUTERLIST Option

The information displayed by the option is described here:

- VLAN - The VID of the VLAN in which the port is an untagged member.
- Port/Trunk ID - The port on the switch where the multicast router is connected. If the switch learned the router on a port trunk, the trunk ID number, not the port number, is displayed.
- Router IP - The IP address of the multicast router.

Examples

The following command displays the current MLD parameter settings:

```
show ipv6 mldsnooping
```

The following command displays a list of active host nodes connected to the switch:

```
show ipv6 mldsnooping hostlist
```

The following command displays a list of active multicast routers:

```
show ipv6 mldsnooping routerlist
```

Equivalent Command

```
show mldsnooping
```

For information, see “SHOW MLDSNOOPING” on page 492.

Chapter 28

Router Redundancy Protocol (RRP) Snooping Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

DISABLE RRPSNOOPING

AlliedWare Plus
Command
Available

Syntax

```
disable rrpsnooping
```

Parameters

None.

Description

This command disables RRP snooping. This is the default setting.

Example

The following command disables RRP snooping:

```
disable rrpsnooping
```

AlliedWare Plus Command

Syntax

```
no ip rrp snooping
```

Modes

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip rrp snooping
```

ENABLE RRPSNOOPING

AlliedWare Plus Command Available

Syntax

```
enable rrpsnooping
```

Parameters

None.

Description

This command enables RRP snooping.

Example

The following command activates RRP snooping on the switch:

```
enable rrpsnooping
```

AlliedWare Plus Command

Syntax

```
ip rrp snooping
```

Modes

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# ip rrp snooping
```

SHOW RRPSNOOPING

AlliedWare Plus Command Available

Syntax

```
show rrpsnooping
```

Parameter

None.

Description

This command displays whether RRP snooping is enabled or disabled.

Example

The following command displays the status of RRP snooping:

```
show rrpsnooping
```

AlliedWare Plus Command

Syntax

```
show ip rrp snooping
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus# show ip rrp snooping
```

Chapter 29

Ethernet Protection Switching Ring (EPSR) Snooping Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

- “DISABLE EPSRSNOOPING” on page 504
- “ENABLE EPSRSNOOPING” on page 505
- “SHOW EPSRSNOOPING” on page 506

DISABLE EPSRSNOOPING

Syntax

```
disable epsrsnooping [controlvlan=vid|vlan_name|all]
```

Parameter

controlvlan Specifies the control VLAN where Ethernet Protected Switching Ring (EPSR) snooping is to be disabled. The VLAN can be identified by its VID or name. A VLAN name is case-sensitive. To disable EPSR snooping on all the control VLANs on the switch, either omit this parameter or specify ALL.

Description

This command disables EPSR snooping on a control VLAN.

Note
Do not disable EPSR on a control VLAN on the master and transit nodes without first disconnecting one of the network cables that form the ring. Without EPSR, your network's performance could be adversely affected from the loop in the network topology.

Example

This command disables EPSR snooping on the VLAN with the VID 22:

```
disable epsrsnooping controlvlan=22
```

This command disables EPSR snooping on all the controls VLANs on the switch:

```
disable epsrsnooping controlvlan=all
```

ENABLE EPSRSNOOPING

Syntax

```
enable epsrsnooping controlvlan=vid|vlan_name
```

Parameter

controlvlan Specifies the control VLAN where Ethernet Protected Switching Ring (EPSR) snooping is to be enabled. The VLAN can be identified by its VID or name. A VLAN name is case-sensitive. You can specify only one control VLAN at a time with this command.

Description

This command activates EPSR snooping on a control VLAN.

Example

This command activates EPSR snooping on the control VLAN with the VID 4:

```
enable epsrsnooping controlvlan=4
```

SHOW EPSRSNOOPING

Syntax

```
show epsrsnooping
```

Parameter

None.

Description

This command displays the status of EPSR snooping.

Example

```
show epsrsnooping
```

Section IV

SNMPv3

This section has the following chapter:

Chapter 30

SNMPv3 Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

- “ADD SNMPV3 USER” on page 511
- “CREATE SNMPV3 ACCESS” on page 514
- “CREATE SNMPV3 COMMUNITY” on page 517
- “CREATE SNMPV3 GROUP” on page 519
- “CREATE SNMPV3 NOTIFY” on page 521
- “CREATE SNMPV3 TARGETADDR” on page 523
- “CREATE SNMPV3 TARGETPARAMS” on page 526
- “CREATE SNMPV3 VIEW” on page 529
- “DELETE SNMPV3 USER” on page 531
- “DESTROY SNMPv3 ACCESS” on page 532
- “DESTROY SNMPv3 COMMUNITY” on page 534
- “DESTROY SNMPv3 GROUP” on page 535
- “DESTROY SNMPv3 NOTIFY” on page 536
- “DESTROY SNMPv3 TARGETADDR” on page 537
- “DESTROY SNMPv3 TARGETPARMS” on page 538
- “DESTROY SNMPV3 VIEW” on page 539
- “PURGE SNMPV3 ACCESS” on page 541
- “PURGE SNMPV3 COMMUNITY” on page 542
- “PURGE SNMPV3 NOTIFY” on page 543
- “PURGE SNMPV3 TARGETADDR” on page 544
- “PURGE SNMPV3 VIEW” on page 545
- “SET SNMPV3 ACCESS” on page 546
- “SET SNMPV3 COMMUNITY” on page 548
- “SET SNMPV3 GROUP” on page 550
- “SET SNMPV3 NOTIFY” on page 552
- “SET SNMPV3 TARGETADDR” on page 554
- “SET SNMPV3 TARGETPARAMS” on page 556
- “SET SNMPV3 USER” on page 558
- “SET SNMPV3 VIEW” on page 560

ADD SNMPV3 USER

AlliedWare Plus
Command
Available

Syntax

```
add snmpv3 user=user [authentication=md5|sha]
authpassword=password privpassword=password
[storagetype=volatile|nonvolatile]
```

Parameters

user — Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

authentication — Specifies the authentication protocol that is used to authenticate this user with an SNMP entity (manager or NMS). If you do not specify an authentication protocol, this parameter is automatically set to None. The options are:

- md5 — The MD5 authentication protocol. SNMPv3 Users are authenticated with the MD5 authentication protocol after a message is received.
- sha — The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

  Note: You must specify the authentication protocol before you specify the authentication password.

authpassword — Specifies a password for the authentication protocol, up to 32 alphanumeric characters. If you specify an authentication protocol, then you must configure an authentication protocol password.

privpassword — Specifies a password for the 3DES privacy, or encryption protocol, up to 32 alphanumeric characters. This is an optional parameter.

Note: If you specify a privacy password, the privacy protocol is set to DES. You must also specify an authentication protocol and password.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table

	entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 User Table entry.

Examples

This command creates an SNMPv3 user with the name “steven142”, an authentication protocol of MD5, an authentication password of “99doublesecret12”, a privacy password of “encrypt178” and a storage type of nonvolatile.

```
add snmpv3 user=steven142 authentication=md5
authpassword=99doublesecret12 privpassword=encrypt178
storagetype=nonvolatile
```

This command creates an SNMPv3 user with the name “77hoa”, an authentication protocol of SHA, an authentication password of “youvegottobekidding88” and a storage type of nonvolatile.

```
add snmpv3 user=77hoa authentication=sha
authpassword=youvegottobekidding88 storagetype=nonvolatile
```

AlliedWare Plus Command

Syntax

```
snmp-server user user auth sha|md5 auth_password
priv=priv_password
```

Mode

Configure mode

Description

This command differs from the standard command as follows:

- You cannot define the storage type. New entries are automatically assigned the storage type of nonvolatile.
- You must include all of the parameters.

Example

This example creates an SNMPv3 user with the name “csmith”, an authentication protocol of MD5, an authentication password of “light224aq”, and a privacy password of “pl567pe”:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server user csmith auth md5
light224aq priv=pl567pe
```

CREATE SNMPV3 ACCESS

AlliedWare Plus Command Available

Syntax

```
create snmpv3 access=access securitymodel=v1|v2c|v3
securitylevel=noauthentication|authentication|
privacy [readview=readview] [writeview=writeview]
[notifyview=notifyview] [storagetype=volatile|nonvolatile]
```

Parameters

access
: Specifies the name of the security group, up to 32 alphanumeric characters.

securitymodel
: Specifies the security model. The options are:

v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.

v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.

v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

securitylevel
: Specifies the security level. The options are:

noauthentication This option provides no authentication protocol and no privacy protocol.

authentication This option provides an authentication protocol, but no privacy protocol.

privacy
: This option provides an authentication protocol and the privacy protocol.

readview
: Specifies a Read View Name that allows the users assigned to this Group Name to view the information specified by the View Table entry. This is an optional parameter. If you do not assign a value to this parameter, then the readview parameter defaults to none.

writeview
: Specifies a Write View Name that allows the users assigned to this Security Group to write, or modify, the information in the specified View Table. This is an optional parameter. If you do not assign a value to this parameter, then the writeview parameter

defaults to none.

notifyview Specifies a Notify View Name that allows the users assigned to this Group Name to send traps permitted in the specified View. This is an optional parameter. If you do not assign a value to this parameter, then the notifyview parameter defaults to none.

storagetype Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile Allows you to save the table entry to the configuration file on the switch.

Description

This command creates SNMPv3 Access Table entries.

Examples

The following command creates a security group called “testengineering” with a security model of SNMPv3 and a security level of privacy. The security group has a read view named “internet,” a write view named private, and a notify view named “internet.” The storage type is nonvolatile storage.

```
create snmpv3 access=testengineering securitymodel=v3
securitylevel=privacy readview=internet writeview=private
notifyview=internet storage=nonvolatile
```

The following command creates a security group called “swengineering” with a security model of SNMPv3 and a security level of authentication. In addition, the security group has a read view named “internet,” a write view named experimental, and a notify view named “mgmt” (management). The storage type group is nonvolatile storage.

```
create snmpv3 access=swengineering securitymodel=v3
securitylevel=authentication readview=internet
writeview=experimental notifyview=mgmt storage=nonvolatile
```

The following command creates a security group called “hwengineering” with a security model of SNMPv3 and a security level of noauthentication. In addition, the security group has a read view named “internet.”

```
create snmpv3 access=hwengineering securitymodel=v3
securitylevel=authentication readview=internet
```

Note
In the above example, the storage type has not been specified. As a result, the storage type for the hwengineering security group is volatile storage.

AlliedWare Plus Command

Syntax

```
snmp-server group access secure noauth|auth|priv read
readview write writeview notify notifyview model=v1|v2c|v3
```

Mode

Configure mode

Description

This command differs from the standard command as follows:

- This command uses the keyword GROUP instead of ACCESS.
- You cannot define the storage type. New entries are automatically assigned the storage type of nonvolatile.
- You must include all of the parameters.
- The parameters must be entered in the order shown above.

Example

This example creates a security group called “sta5west” with a security model of SNMPv3 and a security level of privacy. The security group has a read view named “internet,” a write view named “private,” and a notify view named “internet:”

```
snmp-server group sta5west secure priv read internet write
private notify internet model v3
```

CREATE SNMPV3 COMMUNITY

Syntax

```
create snmpv3 community index=index
communityname=communityname securityname=securityname
transporttag=transporttag
[storagetype=volatile|nonvolatile]
```

Parameters

index
: Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.

communityname
: Specifies a password for this community entry, up to 32 alphanumeric characters.

securityname
: Specifies the name of an SNMPv1 and SNMPv2 user, up to 32 alphanumeric characters.

transporttag
: Specifies the transport tag, up to 32 alphanumeric characters. This is an optional parameter.

storagetype
: Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile
: Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile
: Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Community Table entry.

Examples

The following command creates an SNMP community with an index of 1213 and a community name of “sunnyvale145.” The user is “chitra34” and the transport tag is “testengtag.” The storage type for this community is nonvolatile storage.

```
create snmpv3 community index=1213
communityname=sunnyvale145 securityname=chitra34
transporttag=testengtag storagetype=nonvolatile
```

The following command creates an SNMP community with an index of 95 and a community name of “12sacramento49.” The user is “regina” and the transport tag “trainingtag.” The storage type for this community is nonvolatile storage.

```
create snmpv3 community index=95
communityname=12sacramento49 securityname=regina
transporttag=trainingtag storagetype=nonvolatile
```

CREATE SNMPV3 GROUP

Syntax

```
create snmpv3 group username=username
[securitymodel=v1|v2c|v3] groupname=groupname
[storagetype=volatile|nonvolatile]
```

Parameter

username — Specifies a user name configured in the SNMPv3 User Table.

securitymodel — Specifies the security model of the above user name. The options are:

- v1 — Associates the Security Name, or User Name, with the SNMPv1 protocol.
- v2c — Associates the Security Name, or User Name, with the SNMPv2c protocol.
- v3 — Associates the Security Name, or User Name, with the SNMPv3 protocol.

groupname — Specifies a group name configured in the SNMPv3 Access Table with the access parameter. See “CREATE SNMPV3 ACCESS” on page 514.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 SecurityToGroup Table entry.

Examples

The following command creates the SNMPv3 SecurityToGroup Table entry for a user named Nancy. The security model is set to the SNMPv3 protocol. The group name, or security group, for this user is the “admin” group. The storage type is set to nonvolatile storage.

```
create snmpv3 group username=Nancy securitymodel=v3
groupname=admin storagetype=nonvolatile
```

The following command creates the SNMPv3 SecurityToGroup Table entry for a user named princess. The security model is set to the SNMPv3 protocol. The group name, or security group, for this user is the “training” group. The storage type is set to nonvolatile storage.

```
create snmpv3 group username=princess securitymodel=v3
groupname=training storagetype=nonvolatile
```

CREATE SNMPV3 NOTIFY

AlliedWare Plus Command Available

Syntax

```
create snmpv3 notify=notify tag=tag [type=trap|inform]
[storagetype=volatile|nonvolatile]
```

Parameters

notify: Specifies the name of an SNMPv3 Notify Table entry, up to 32 alphanumeric characters.

tag: Specifies the notify tag name, up to 32 alphanumeric characters. This is an optional parameter.

type: Specifies the message type. This is an optional parameter. The options are:

- trap — Trap messages are sent, with no response expected from another entity (NMS or manager). This is the default.
- inform — Inform messages are sent, with a response expected from another entity (NMS or manager).

storagetype: Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Notify Table entry.

Examples

The following command creates the SNMPv3 Notify Table entry called “testengtrap1” and the notify tag is “testengtag1.” The message type is defined as a trap message and the storage type for this entry is nonvolatile storage.

```
create snmpv3 notify=testengtrap1 tag=testengtag1 type=trap
storagetype=nonvolatile
```

The following command creates the SNMPv3 Notify Table entry called “testenginform5” and the notify tag is “testenginformtag5.” The message type is defined as an inform message and the storage type for this entry is nonvolatile storage.

```
create snmpv3 notify=testenginform5 tag=testenginformtag5
type=inform storagetype=nonvolatile
```

AlliedWare Plus Command

Syntax

snmp-server notify *notify* tag *tag* type trap|inform

Mode

Configure mode

Description

This command differs from the standard command as follows:

- ❒ You cannot define the storage type. New entries are automatically assigned the storage type of nonvolatile.
- ❒ You must include all of the parameters.
- ❒ The parameters must be entered in the order shown above.

Example

The following command creates an SNMPv3 Notify Table entry called “testwesttrap1”. The notify tag is “testwesttag1” and the message type is defined as a trap message:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server notify testwesttrap1 tag
testwesttag1 type trap
```

CREATE SNMPV3 TARGETADDR

AlliedWare Plus Command Available

Syntax

```
create snmpv3 targetaddr=targetaddr params=params
ipaddress=ipaddress udpport=udpport timeout=timeout
retries=retries taglist=taglist
[storagetype=volatile|nonvolatile]
```

Parameters

targetaddr
Specifies the name of the SNMP manager, or host, that manages the SNMP activity on the switch, up to 32 alphanumeric characters.

params
Specifies the target parameters name, up to 32 alphanumeric characters.

ipaddress
Specifies the IP address of the host.

udpport
Specifies the UDP port in the range of 0 to 65535. The default UDP port is 162. This is an optional parameter.

timeout
Specifies the timeout value in milliseconds. The range is 0 to 2,147,483,647 milliseconds, and the default is 1500 milliseconds. This is an optional parameter.

retries
Specifies the number of times the switch resends an inform message. The default is 3. This is an optional parameter.

taglist
Specifies a tag or list of tags, up to 256 alphanumeric characters. Use a space to separate entries. This is an optional parameter.

storagetype
Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile
Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile
Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Target Address Table entry.

Examples

In the following command, the name of the Target Address Table entry is “snmphost1.” In addition, the params parameter is assigned to “snmpv3manager” and the IP address is 198.1.1.1. The tag list consists of “swengtag,” “hwengtag,” and “testengtag.” The storage type for this table entry is nonvolatile storage.

```
create snmpv3 targetaddr=snmphost1 params=snmpv3manager
ipaddress=198.1.1.1 taglist=swengtag,hwengtag,testengtag
storagetype=nonvolatile
```

In the following command, the name of the Target Address Table entry is snmphost99. The params parameter is “snmpmanager7” and the IP address is 198.1.2.2. The tag list is “trainingtag.” The storage type for this table entry is nonvolatile storage.

```
create snmpv3 targetaddr=snmphost99 params=snmpmanager7
ipaddress=198.1.2.2 taglist=trainingtag
storagetype=nonvolatile
```

AlliedWare Plus Command

Syntax

```
snmp-server targetaddr targetaddr param params ipaddress
ipaddress tag taglist udpport udpport timeout timeout
retries retries
```

Mode

Configure mode

Description

This command differs from the standard command as follows:

- ❐ You cannot define the storage type. New entries are automatically assigned the storage type of nonvolatile.
- ❐ You must include all of the parameters.
- ❐ The parameters must be entered in the order shown above.

Example

In this example, the name of the Target Address Table entry is “snmphost1.” The params parameter is assigned to “snmpv3manager” and the IP address is 198.1.1.1. The tag list consists of “swengtag,” “hwengtag,” and “testengtag.” The default values are used for the other parameters:

```
awplus> enable
awplus# configure terminal
```

```
awplus(config)# snmp-server targetaddr snmpv3host1 param
snmpv3manager ipaddress 198.1.1.1 tag
swengtag,hwengtag,testengtag udpport 162 timeout 1500
retries 3
```

CREATE SNMPV3 TARGETPARAMS

AlliedWare Plus
Command
Available

Syntax

```
create snmpv3 targetparams=targetparams username=username
[securitymodel=v1|v2c|v3] [messageprocessing=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] [storagetype=volatile|nonvolatile]
```

Parameters

targetparams — Specifies the name of the SNMPv3 Target Parameters Table entry, up to 32 alphanumeric characters.

username — Specifies a user name configured in the SNMPv3 User Table.

securitymodel — Specifies the security model of the above user name. The options are:

- v1 — Associates the User Name, or Security Name, with the SNMPv1 protocol.
- v2c — Associates the User Name, or Security Name, with the SNMPv2c protocol.
- v3 — Associates the User Name, or Security Name, with the SNMPv3 protocol.

messageprocessing — Specifies the SNMP protocol that is used to process, or send messages. The options are:

- v1 — Messages are processed with the SNMPv1 protocol.
- v2c — Messages are processed with the SNMPv2c protocol.
- v3 — Messages are processed with the SNMPv3 protocol.

securitylevel — Specifies the security level. The options are:

- noauthentication — This option provides no authentication protocol and no privacy protocol.
- authentication — This option provides an authentication protocol, but no privacy protocol.

privacy — This option provides an authentication protocol and the privacy protocol.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 Target Parameters Table entry.

Examples

In the following command, the Target Parameters Table entry is called “snmpv3mgr13” and user name is “user444.” The security model is set to the SNMPv3 protocol. In addition, the security level is set to privacy and the storage type is nonvolatile.

```
create snmpv3 targetparams=snmpv3mgr13 username=user444
securitymodel=v3 messageprocessing=v3 securitylevel=privacy
storagetype=nonvolatile
```

In the following command, the Target Parameters Table entry is called “snmpmanager” and the user name is “pat365.” The security model is set to SNMPv3 protocol. In addition, the security level is set to authentication and the storage type is nonvolatile.

```
create snmpv3 targetparams=snmpmanager username=pat365
securitymodel=v3 messageprocessing=v3
securitylevel=authentication storagetype=nonvolatile
```

AlliedWare Plus Command

Syntax

```
snmp-server targetparams targetparams user username secure
noauth|auth|priv model v1|v2c|v3 message v1|v2c|v3
```

Mode

Configure mode

Description

This command differs from the standard command as follows:

- ❒ You cannot define the storage type. New entries are automatically assigned the storage type of nonvolatile.
- ❒ You must include all of the parameters.
- ❒ The parameters must be entered in the order shown above.

Example

In this example, the Target Parameters Table entry is called “snmpv3mgr24” and the user name is “user444.” The security level is set to authentication, the security model to the SNMPv3 protocol, and the message processing to SNMPv3.

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server targetparams snmpv3mgr24 user
user444 secure auth model v3 message v3
```

CREATE SNMPV3 VIEW

AlliedWare Plus Command Available

Syntax

```
create snmpv3 view=view [subtree=OID|text] mask=mask
[type=included|excluded]
[storagetype=volatile|nonvolatile]
```

Parameters

view — Specifies the name of the view, up to 32 alphanumeric characters.

subtree — Specifies the view of the MIB Tree. The options are:

- OID — A numeric value in hexadecimal format.
- text — Text name of the view.

mask — Specifies the subtree mask, in hexadecimal format.

type — Specifies the view type. This is an optional parameter. The options are:

- included — Permits a user to view the specified subtree. This is the default.
- excluded — Does not permit a user to view the specified subtree.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command creates an SNMPv3 View Table entry.

Examples

The following command creates an SNMPv3 View Table entry called "internet1" with a subtree value of the Internet MIBs and a view type of included. The storage type for this table entry is nonvolatile storage.

```
create snmpv3 view=internet1 subtree=internet type=included
storagetype=nonvolatile
```

The following command creates an SNMPv3 View Table entry called “tcp1” with a subtree value of the TCP/IP MIBs and a view type of excluded. The storage type for this table entry is nonvolatile storage.

```
create snmpv3 view=tcp1 subtree=tcp type=excluded
storagetype=nonvolatile
```

AlliedWare Plus Command

Syntax

```
snmp-server view view subtree OID|text mask mask type
included|excluded
```

Mode

Configure mode

Description

This command differs from the standard command as follows:

- You cannot define the storage type. New entries are automatically assigned the storage type of nonvolatile.
- You must include all of the parameters.
- The parameters must be entered in the order shown above.

Example

This example creates an SNMPv3 View Table entry called “internet1” with a subtree value of the Internet MIBs, a mask of 1, and a view type of included:

```
awplus> enable
awplus# configure terminal
awplus(config)# snmp-server view internet1 subtree internet
mask 1 type included
```

DELETE SNMPV3 USER

AlliedWare Plus Command Available

Syntax

```
delete snmpv3 user=user
```

Parameters

user	Specifies the name of an SNMPv3 user to delete from the switch.

Description

This command deletes SNMPv3 User Table entries. After you delete an SNMPv3 user from the switch, you cannot recover it.

Examples

The following command deletes the user named “wilson890.”

```
delete snmpv3 user=wilson890
```

The following command deletes the user named “75murthy75.”

```
delete snmpv3 user=75murthy75
```

AlliedWare Plus Command

Syntax

```
no snmp-server user user
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes an SNMPv3 User Table entry called “rs12eng”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server user rs12eng
```

DESTROY SNMPv3 ACCESS

Syntax

```
destroy snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy]
```

Parameter

access Specifies an SNMPv3 Access Table entry.

securitymodel Specifies the security model of the user name specified above. The options are:

v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.

v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.

v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

securitylevel Specifies the security level. The options are:

noauthentication This option provides no authentication protocol and no privacy protocol.

authentication This option provides an authentication protocol, but no privacy protocol.

privacy This option provides an authentication protocol and the privacy protocol.

Description

This command deletes an SNMPv3 Access Table entry. After you delete an SNMPv3 Access Table entry, you cannot recover it.

Examples

The following command deletes the SNMPv3 Access Table entry called “swengineering” with a security model of the SNMPv3 protocol and a security level of authentication.

```
destroy snmpv3 access=swengineering securitymodel=v3
securitylevel=authentication
```

The following command deletes the SNMPv3 Access Table entry called “testengineering” with a security model of the SNMPv3 protocol and a security level of privacy.

```
destroy snmpv3 access=testengineering securitymodel=v3
securitylevel=privacy
```

DESTROY SNMPv3 COMMUNITY

Syntax

```
destroy snmpv3 community index=index
```

Parameter

index Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.

Description

This command deletes an SNMPv3 Community Table entry. After you delete an SNMPv3 Community Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 Community Table entry with an index of 1001.

```
destroy snmpv3 community index=1001
```

The following command deletes an SNMPv3 Community Table entry with an index of 5.

```
destroy snmpv3 community index=5
```

DESTROY SNMPv3 GROUP

Syntax

```
destroy snmpv3 group username=username
[securitymodel=v1|v2c|v3]
```

Parameter

username	Specifies a user name configured in the SNMPv3 User Table.
securitymodel	Specifies the security model of the above user name. The options are:

v1	Associates the Security Name, or User Name, with the SNMPv1 protocol.
v2c	Associates the Security Name, or User Name, with the SNMPv2c protocol.
v3	Associates the Security Name, or User Name, with the SNMPv3 protocol.

Description

This command deletes an SNMPv3 SecurityToGroup Table entry. After you delete an SNMPv3 SecurityToGroup Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 User Table entry for a user called Dave with an security model of the SNMPv3 protocol:

```
destroy snmpv3 group username=Dave securitymodel=v3
```

The following command deletes an SNMPv3 User Table entry for a user called May with an security model of the SNMPv3 protocol:

```
destroy snmpv3 group username=May securitymodel=v3
```

DESTROY SNMPv3 NOTIFY

AlliedWare Plus
Command
Available

Syntax

```
destroy snmpv3 notify=notify
```

Parameter

notify	Specifies an SNMPv3 Notify Table entry.

Description

This command deletes SNMPv3 Notify Table entries. After you delete an SNMPv3 Notify Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 Notify Table entry called “systemtestnotifytrap.”

```
destroy snmpv3 notify=systemtestnotifytrap
```

The following command deletes an SNMPv3 Notify Table entry called “engineeringinform1.”

```
destroy snmpv3 notify=engineeringinform1
```

AlliedWare Plus Command

Syntax

```
no snmp-server notify notify
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes an SNMPv3 Notify Table entry called “testwesttrap1”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server notify testwesttrap1
```

DESTROY SNMPv3 TARGETADDR

AlliedWare Plus Command Available

Syntax

```
destroy snmpv3 targetaddr=target
```

Parameter

targetaddr Specifies an SNMPv3 Target Address table entry.

Description

This command deletes an SNMPv3 Target Address Table entry. After you delete an SNMPv3 Target Address Table entry, you cannot recover it.

Example

The following command deletes an SNMPv3 Address Table entry called “snmpmanager.”

```
destroy snmpv3 targetaddr=snmpmanager
```

AlliedWare Plus Command

Syntax

```
no snmp-server targetaddr target
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes an SNMPv3 Target Address Table entry called “snmpv3host5”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server targetaddr snmpv3host5
```

DESTROY SNMPv3 TARGETPARMS

AlliedWare Plus
Command
Available

Syntax

```
destroy snmpv3 targetparams=targetparams
```

Parameter

targetparams — Specifies an SNMPv3 Target Parameters table entry.

Description

This command deletes SNMPv3 Target Parameters Table entries. After you delete an SNMPv3 Target Parameters Table entry, you cannot recover it.

Examples

The following command deletes an SNMPv3 Target Parameters Table entry called “targetparameter1.”

```
destroy snmpv3 targetparams=targetparameter1
```

The following command deletes an SNMPv3 Target Parameters Table entry called “snmpmanager.”

```
destroy snmpv3 targetparams=snmpmanager
```

AlliedWare Plus Command

Syntax

```
no snmp-server targetparams target
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes an SNMPv3 Target Parameters Table entry called “mgrsnmpv3params”:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server targetparams mgrsnmpv3params
```

DESTROY SNMPV3 VIEW

AlliedWare Plus
Command
Available

Syntax

```
destroy snmpv3 view=view [subtree=OID|text]
```

Parameters

view Specifies the name of the view, up to 32 alphanumeric characters.

subtree Specifies the view subtree view. The options are:

OID A numeric value in hexadecimal format.

text Text name of the view.

Description

This command deletes SNMPv3 View Table entries. After you delete an SNMPv3 View Table entry, you cannot recover it.

Examples

The following command deletes the SNMPv3 View Table entry named “experimental.“ The subtree value of this table entry is experimental.

```
destroy snmpv3 view=experimental subtree=experimental
```

The following command deletes the SNMPv3 View Table entry named “directory.” The subtree value of this table entry is 1.3.6.1.3.

```
destroy snmpv3 view=directory subtree=1.3.6.1.3
```

AlliedWare Plus Command

Syntax

```
no snmp-server view view subtree OID|text
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes an SNMPv3 View Table entry called “internet1” with a subtree value of the Internet MIBs:

```
awplus> enable
awplus# configure terminal
awplus(config)# no snmp-server view internet1 subtree
internet
```

PURGE SNMPV3 ACCESS

Syntax

```
purge snmpv3 access
```

Parameters

None

Description

This command resets the SNMPv3 Access Table to its default value by removing all the access table entries. To remove a single entry, use “DESTROY SNMPv3 ACCESS” on page 532.

Example

The following example removes all the SNMPv3 Access Table entries:

```
purge snmpv3 access
```

PURGE SNMPV3 COMMUNITY

Syntax

```
purge snmpv3 community
```

Parameters

None

Description

This command resets the SNMPv3 Community Table to its default value by removing all the community table entries. To remove a single entry, use “DESTROY SNMPv3 COMMUNITY” on page 534.

Example

The following example removes all the SNMPv3 Community Table entries:

```
purge snmpv3 community
```

PURGE SNMPV3 NOTIFY

Syntax

```
purge snmpv3 notify
```

Parameters

None

Description

This command resets the SNMPv3 Notify Table to its default value by removing all the notify table entries. To remove a single entry, use "DESTROY SNMPv3 NOTIFY" on page 536.

Example

The following example removes all the entries from the SNMPv3 Notify Table:

```
purge snmpv3 notify
```

PURGE SNMPV3 TARGETADDR

Syntax

```
purge snmpv3 targetaddr
```

Parameters

None

Description

This command resets the SNMPv3 Target Address Table to its default values by removing all the target address table entries. To remove a single entry, use “DESTROY SNMPv3 TARGETADDR” on page 537.

Example

The following example removes all the entries from the SNMPv3 Target Address Table:

```
purge snmpv3 targetaddr
```

PURGE SNMPV3 VIEW

Syntax

```
purge snmpv3 view
```

Parameters

None

Description

This command resets the SNMPv3 View Table to its default values by removing all the view table entries. To remove a single entry, use “DESTROY SNMPV3 VIEW” on page 539.

Example

The following example removes all the entries from the SNMPv3 View Table:

```
purge snmpv3 view
```

SET SNMPV3 ACCESS

Syntax

```
set snmpv3 access=access [securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] readview=readview writeview=writeview
notifyview=notifyview [storagetype=volatile|nonvolatile]
```

Parameters

access
Specifies the name of the group, up to 32 alphanumeric characters.

securitymodel
Specifies the security model. Options are:

v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.

v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.

v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

securitylevel
Specifies the security level. The options are:

noauthentication This option provides no authentication protocol and no privacy protocol.

authentication This option provides an authentication protocol, but no privacy protocol.

privacy This option provides an authentication protocol and the privacy protocol.

readview
Specifies a Read View Name that allows the users assigned to this Group Name to view the information specified by the View Table entry.

writeview
Specifies a Write View Name that allows the users assigned to this Security Group to write, or modify, the information in the specified View Table.

notifyview
Specifies a Notify View Name that allows the users assigned to this Group Name to send traps permitted in the specified View.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Access Table entry.

Examples

The following command modifies the group called engineering. The new read view is the Internet MIBs and the storage type is volatile storage.

```
set snmpv3 access=engineering securitymodel=v3
securitylevel=authentication readview=internet
storagetype=volatile
```

The following command modifies the group called training. The read view, write view, and notify view are set to the Internet MIBs. The storage type is nonvolatile storage.

```
set snmpv3 access=training securitymodel=v3
securitylevel=privacy readview=internet writeview=internet
notifyview=internet storagetype=nonvolatile
```

SET SNMPV3 COMMUNITY

Syntax

```
set snmpv3 community index=index communityname=communityname
securityname=securityname transporttag=transporttag
[storagetype=volatile|nonvolatile]
```

Parameters

index — Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.

communityname — Specifies a password of this community, up to 32 alphanumeric characters.

securityname — Specifies the name of an SNMPv1 and SNMPv2 user, up to 32 alphanumeric characters.

transporttag — Specifies the transport tag, up to 32 alphanumeric characters.

storagetype — Specifies the storage type of this table entry. This is an optional parameter. The options are:

- volatile — Does not allow you to save the table entry to the configuration file on the switch. This is the default.
- nonvolatile — Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Community Table entry.

Examples

The following command modifies the community table entry with an index of 1001. The community has a password of “secretpassword98” and a security name of “user451.” The transport tag is set to “sampletag4” and the storage type is set to nonvolatile storage.

```
set snmpv3 community index=1001
communityname=secretpassword98 securityname=user451
transporttag=sampletag4 storagetype=nonvolatile
```

The following command modifies the community table entry with an index of 52. The community has a password of “oldmiss71” and a security name of “jjhuser234.” The transport tag is set to “testtag40.”

```
set snmpv3 community index=52 communityname=oldmiss71
securityname=jjhuser234 transporttag=testtag40
```

SET SNMPV3 GROUP

Syntax

```
set snmpv3 group username=username [securitymodel=v1|v2c|v3]
groupname=groupname [storagetype=volatile|nonvolatile]
```

Parameter

username Specifies a user name configured in the SNMPv3 User Table.

securitymodel Specifies the security model of the above user name. The options are:

v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.

v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.

v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

groupname Specifies a group name configured in the SNMPv3 Access Table.

storagetype Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 SecurityToGroup Table entry.

Examples

The following command modifies the SecurityToGroup Table entry with a user name of “nancy28.” The security model is the SNMPv3 protocol. and the group name is set to engineering.

```
set snmpv3 group username=nancy28 securitymodel=v3
groupname=engineering
```

The following command modifies the SecurityToGroup Table entry with a user name of “nelvid.” The security model is the SNMPv3 protocol and the group name “systemtest.”

```
set snmpv3 group username=nelvid securitymodel=v3
groupname=systemtest
```

SET SNMPV3 NOTIFY

Syntax

```
set snmpv3 notify=notify tag=tag [type=trap|inform]
[storagetype=volatile|nonvolatile]
```

Parameters

notify
Specifies the name associated with the trap message, up to 32 alphanumeric characters.

tag
Specifies the notify tag name, up to 32 alphanumeric characters.

type
Specifies the message type. Options are:

trap
Trap messages are sent, with no response expected from the host.

inform
Inform messages are sent, with a response expected from the host.

storagetype
Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile
Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile
Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Notify Table entry.

Examples

The following command modifies an SNMPv3 Notify Table entry called “systemtesttrap2.” The notify tag is “systemtesttag2” and the message type is a trap message.

```
set snmpv3 notify=systemtesttrap2 tag=systemtesttag2
type=trap
```

The following command modifies an SNMPv3 Notify Table entry called “systemtestinform5.” The notify tag is “systemtestinform5tag” and the message type is an inform message.

```
set snmpv3 notify=systemtestinform5 tag=systemtestinform5tag
type=inform
```

SET SNMPV3 TARGETADDR

Syntax

```
set snmpv3 targetaddr=targetaddr params=params
ipaddress=ipaddress udpport=udpport timeout=timeout
retries=retries taglist=taglist
[storagetype=volatile|nonvolatile]
```

Parameters

targetaddr
Specifies the name of the SNMP entity (NMS or manager) that manages the SNMP activity on the switch, up to 32 alphanumeric characters.

params
Specifies the target parameters name, up to 32 alphanumeric characters. This is an optional parameter.

ipaddress
Specifies the IP address of the host. This is an optional parameter.

udpport
Specifies the UDP port in the range of 0 to 65535. The default UDP port is 162. This is an optional parameter.

timeout
Specifies the timeout value in milliseconds. The range is 0 to 2,147,483,647 milliseconds, and the default is 1500 milliseconds. This is an optional parameter.

retries
Specifies the number of times the switch retries to send an inform message. The default is 3. This is an optional parameter.

taglist
Specifies a tag or list of tags, up to 256 alphanumeric characters. Use a space to separate entries. This is an optional parameter.

storagetype
Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile
Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile
Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 Target Address Table entry.

Examples

The following command modifies the Target Address Table entry with a value of “snmphost.” The params parameter is set to “targetparameter7” and the IP address is 198.1.1.1. The taglist is set to “systemtesttraptag” and “systemtestinformtag.”

```
set snmpv3 targetaddr=snmphost params=targetparameter7
ipaddress=198.1.1.1 taglist=systemtesttraptag
systemtestinformtag
```

The following command modifies the Target Address Table entry with a value of “host.” The params parameter is set to “targetparameter22” and the IP address is 198.1.1.198. The taglist is set to “engineeringtraptag” and “engineeringinformtag.”

```
set snmpv3 targetaddr=host params=targetparameter22
ipaddress=198.1.1.198 taglist=engineeringtraptag
engineeringinformtag
```

SET SNMPV3 TARGETPARAMS

Syntax

```
set snmpv3 targetparams=targetparams username=username
[securitymodel=v1|v2c|v3] [messageprocessing=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] [storagetype=volatile|nonvolatile]
```

Parameters

targetparams
Specifies the target parameters name, up to 32 alphanumeric characters.

username
Specifies the user name.

securitymodel
Specifies the security model of the above user name. The options are:

v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.

v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.

v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

messageprocessing
Specifies the SNMP protocol that is used to process, or send messages. Configure this parameter only if you have selected the SNMPv1 or SNMPv2c protocols as the security model. If you have selected the SNMPv3 protocol as the security model, message processing is automatically set to the SNMPv3 protocol. The options are:

v1 Messages are processed with the SNMPv1 protocol.

v2c Messages are processed with the SNMPv2c protocol.

v3 Messages are processed with the SNMPv3 protocol.

securitylevel
Specifies the security level. The options are:

noauthentication This option provides no authentication protocol and no privacy protocol.

authentication This option provides an authentication protocol, but no privacy protocol.

privacy This option provides an authentication protocol and the privacy protocol.

storagetype Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies a Target Parameters Table entry.

Examples

The following command modifies the Target Parameters Table entry called "host23." The user name is "user7990" and the security model is the SNMPv3 protocol. The security level is set to the privacy level.

```
set snmpv3 targetparams=host23 username=loan1
securitymodel=v3 securitylevel=privacy
```

The following command modifies the Target Parameters Table entry called "manager9". The user name is "loan1" and the security model is the SNMPv3 protocol. The security level is set to the authentication protocol.

```
set snmpv3 targetparams=manager9 username=loan1
securitymodel=v3 securitylevel=authentication
```

SET SNMPV3 USER

Syntax

```
set snmpv3 user=user [authentication=md5|sha]
authpassword=password privpassword=password
[storagetype=volatile|nonvolatile]
```

Parameters

user
: Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

authentication
: Specifies the authentication protocol that is used to authenticate this user with an SNMPv3 entity (or NMS). The default is no authentication. The options are:

md5	The MD5 authentication protocol. Users are authenticated with the MD5 authentication protocol after a message is received.
sha	The SHA authentication protocol. Users are authenticated with the SHA authentication protocol after a message is received.

authpassword
: Specifies a password for the authentication protocol, up to 32 alphanumeric characters.

privpassword
: Specifies a password for the 3DES privacy, or encryption protocol, up to 32 alphanumeric characters. Configuring a privacy protocol password, turns on the DES privacy protocol.

storagetype
: Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile	Does not allow you to save the table entry to the configuration file on the switch. This is the default.
nonvolatile	Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 User Table entry.

Examples

The following command modifies a User Table entry called “atiuser104”. The authentication protocol is set to the MD5 protocol and the authentication password is “atlanta45denver.” The DES privacy protocol is on and the privacy password is “denvertoatlanta3.”

```
set snmpv3 user=atiuser104 authentication=md5
authpassword=atlanta45denver privpassword=denvertoatlanta3
```

The following command modifies a User Table entry called “atiuser104.” The authentication protocol is set to the MD5 protocol and the authentication password is “nycbostonwash56.” The privacy protocol is on and the privacy password is “bostontoamherst7.” The storage type is set to nonvolatile storage.

```
set snmpv3 user=atiuser104 authentication=md5
authpassword=nycbostonwash56 privpassword=bostontoamherst7
storagetype=nonvolatile
```

SET SNMPV3 VIEW

Syntax

```
set snmpv3 view=view [subtree=OID|text] mask=mask
[type=included|excluded]
[storagetype=volatile|nonvolatile]
```

Parameters

view
Specifies the name of the view, up to 32 alphanumeric characters.

subtree
Specifies the view subtree view. Options are:

OID
A numeric value in hexadecimal format.

text
Text name of the view.

mask
Specifies the subtree mask, in hexadecimal format.

type
Specifies the view type. Options are:

included
Permits the user assign to this View Name to see the specified subtree.

excluded
Does not permit the user assigned to this View Name to see the specified subtree.

storagetype
Specifies the storage type of this table entry. This is an optional parameter. The options are:

volatile
Does not allow you to save the table entry to the configuration file on the switch. This is the default.

nonvolatile
Allows you to save the table entry to the configuration file on the switch.

Description

This command modifies an SNMPv3 View Table entry.

Examples

The following command modifies the view called “internet1.” The subtree is set to the Internet MIBs and the view type is included.

```
set snmpv3 view=internet1 subtree=internet type=included
```

The following command modifies the view called system. The subtree is set to 1.3.6.1.2.1 (System MIBs) and the view type is excluded.

```
set snmpv3 view=system subtree=1.3.6.1.2.1 type=excluded
```

SHOW SNMPV3 ACCESS

AlliedWare Plus Command Available

Syntax

```
show snmpv3 access[=access]
```

Parameter

access	Specifies an SNMPv3 Access Table entry.

Description

This command displays the SNMPv3 Access Table. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 Access Table entry called “production.”

```
show snmpv3 access=production
```

The following command displays all of the SNMPv3 Access Table entries:

```
show snmpv3 access
```

AlliedWare Plus Command

Syntax

```
show snmp-server group
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the entire SNMPv3 Access Table. This command differs from the standard command in that it uses the keyword GROUP instead of ACCESS and that it does not let you display individual entries.

Example

```
awplus# show snmp-server group
```

SHOW SNMPV3 COMMUNITY

Syntax

```
show snmpv3 community index=index
```

Parameter

index	Specifies the name of this SNMPv3 Community Table entry, up to 32 alphanumeric characters.

Description

This command displays the SNMPv3 Community Table. You can display one or all of the SNMPv3 Community Table entries.

Examples

The following command displays the Community Table entry with an index of 246:

```
show snmpv3 community index=246
```

The following command displays all of the Community Table entries:

```
show snmpv3 community
```

SHOW SNMPv3 GROUP

Syntax

```
show snmpv3 group [username=username]
[securitymodel=v1|v2c|v3]
```

Parameter

username Specifies a user name configured in the SNMPv3 User Table.

securitymodel Specifies the security model of the above user name. The options are:

v1 Associates the Security Name, or User Name, with the SNMPv1 protocol.

v2c Associates the Security Name, or User Name, with the SNMPv2c protocol.

v3 Associates the Security Name, or User Name, with the SNMPv3 protocol.

Description

This command displays SNMPv3 SecurityToGroup Table entries. You can display one or all of the table entries.

Example

The following command displays the SNMPv3 SecurityToGroup Table entry for a user named Dave who is assigned a security model of the SNMPv3 protocol.

```
show snmpv3 group username=Dave securitymodel=v3
```

The following command displays all of the SNMPv3 SecurityToGroup Table entries:

```
show snmpv3 group
```

SHOW SNMPV3 NOTIFY

AlliedWare Plus Command Available

Syntax

```
show snmpv3 notify[=notify]
```

Parameter

notify	Specifies an SNMPv3 Notify Table entry.

Description

This command displays SNMPv3 Notify Table entries. You can display one or all of the table entries.

Examples

The following command displays all of the SNMPv3 Notify Table entries:

```
show snmpv3 notify
```

The following command displays the SNMPv3 Notify Table entry called "testengtrap1":

```
show snmpv3 notify=testengtrap1
```

AlliedWare Plus Command

Syntax

```
show snmp-server notify
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the entire SNMPv3 Notify Table. You cannot specify an individual entry as you can with the standard command.

Example

```
awplus# show snmp-server notify
```

SHOW SNMPV3 TARGETADDR

AlliedWare Plus
Command
Available

Syntax

```
show snmpv3 targetaddr[=targetaddr]
```

Parameter

targetaddr Specifies an SNMPv3 Target Address Table entry.

Description

This command displays SNMPv3 Target Address Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 Target Address Table entry called “snmpv3host55”:

```
show snmpv3 targetaddr=snmpv3host55
```

The following command displays all of the SNMPv3 Target Address Table entries:

```
show snmpv3 targetaddr
```

AlliedWare Plus Command

Syntax

```
show snmp-server targetaddr
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the entire SNMPv3 Target Address Table. You cannot specify an individual entry as you can with the standard command.

Example

```
awplus# show snmp-server targetaddr
```

SHOW SNMPV3 TARGETPARAMS

AlliedWare Plus
Command
Available

Syntax

```
show snmpv3 targetparams[=targetparams]
```

Parameter

targetparams	Specifies an SNMPv3 Target Parameters Table entry.

Description

This command displays SNMPv3 Target Parameters Table entries. You can display one or all of the table entries.

Examples

The following command displays the entire SNMPv3 Target Parameters Table:

```
show snmpv3 targetparams
```

The following command displays the SNMPv3 Target Parameters Table entry called “snmpv3manager95”:

```
show snmpv3 targetparams=snmpv3manager95
```

AlliedWare Plus Command

Syntax

```
show snmp-server targetparams
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the entire SNMPv3 Target Parameters Table. Unlike the standard command it does not allow you to specify an individual entry.

Example

```
awplus# show snmp-server targetparams
```

SHOW SNMPV3 USER

AlliedWare Plus Command Available

Syntax

```
show snmpv3 user[=user]
```

Parameters

user — Specifies the name of an SNMPv3 user, up to 32 alphanumeric characters.

Description

This command displays SNMPv3 User Table entries. You can display one or all of the table entries.

Examples

The following command displays all of the SNMPv3 User Table entries:

```
show snmpv3 user
```

The following command displays the SNMPv3 User Table entry for a user name of Robert:

```
show snmpv3 user=Robert
```

AlliedWare Plus Command

Syntax

```
show snmp-server user
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays all of the entries in the SNMPv3 User Table. You cannot specify an individual entry as you can with the standard command.

Example

```
awplus# show snmp-server user
```

SHOW SNMPV3 VIEW

AlliedWare Plus Command Available

Syntax

```
show snmpv3 view[=view] [subtree=OID|text]
```

Parameter

view — Specifies an SNMPv3 View Table entry.

subtree — Specifies the view subtree view. Options are:

OID	A numeric value in hexadecimal format.
text	Text name of the view.

Description

This command displays the SNMPv3 View Table entries. You can display one or all of the table entries.

Examples

The following command displays the SNMPv3 View Table entry called “snmpv3manager95”:

```
show snmpv3 view=snmpv3manager95
```

The following command displays all the SNMPv3 View Table entries:

```
show snmpv3 view
```

AlliedWare Plus Command

Syntax

```
show snmp-server view
```

Mode

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays the entire SNMPv3 View Table. Unlike the standard command, it does not let you specify an individual entry or a subtree.

Example

```
awplus# show snmp-server view
```

Section V

Spanning Tree Protocols

This section has the following chapters:

Chapter 31

Spanning Tree Protocol (STP) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ACTIVATE STP

AlliedWare Plus
Command
Available

Syntax

```
activate stp
```

Parameters

None.

Description

Use this command to designate STP as the active spanning tree. You cannot enable STP or configure its parameters until you have designated it as the active spanning tree with this command.

Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on a switch or a stack at a time.

Example

This command designates STP as the active spanning tree:

```
activate stp
```

AlliedWare Plus Command

Syntax

```
spanning-tree mode stp
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode stp
```

DISABLE STP

AlliedWare Plus
Command
Available

Syntax

```
disable stp
```

Parameters

None.

Description

This command disables the Spanning Tree Protocol. To view the current status of STP, refer to “SHOW STP” on page 586. The default setting for STP is disabled.

Example

The following command disables STP:

```
disable stp
```

AlliedWare Plus Command

Syntax

```
no spanning-tree stp enable bridge-forward
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree stp enable bridge-forward
```

ENABLE STP

AlliedWare Plus Command Available

Syntax

```
enable stp
```

Parameters

None.

Description

This command enables the Spanning Tree Protocol. To view the current status of STP, refer to “SHOW STP” on page 586. The default setting for STP is disabled.

> **Note**
> You cannot enable STP until after you have activated it with “ACTIVATE STP” on page 574.

Example

The following command enables STP:

```
enable stp
```

AlliedWare Plus Command

Syntax

```
spanning-tree stp enable
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree stp enable
```

PURGE STP

Syntax

```
purge stp
```

Parameters

None.

Description

This command returns all the STP bridge and port parameters to the default settings. STP must be disabled in order for you to use this command. To disable STP, see “DISABLE STP” on page 575.

Example

The following command resets the STP parameter settings to their default values:

```
purge stp
```

Equivalent Command

```
set stp default
```

For information, see “SET STP” on page 578.

SET STP

AlliedWare Plus Command Available

Syntax

```
set stp [default] [priority=priority] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
```

Parameters

default — Disables STP and returns all bridge and port STP settings to the default values. This parameter cannot be used with any other command parameter and can only be used when STP is disabled. (This parameter performs the same function as the PURGE STP command.)

priority — Specifies the priority number for the bridge. This number is used in determining the root bridge for STP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge.

The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 12. You specify the increment that represents the desired bridge priority value. The default value is 32,768 (increment 8).

Table 12. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

hellotime Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

forwarddelay Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, all links may not have had time to adapt to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds.

maxage Specifies the length of time after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default 20, all bridges delete current configuration messages after 20 seconds. The range is 6 to 40 seconds. The default is 20 seconds.

Note
The value for the maxage parameter must be greater than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

Description

This command sets the following STP parameters:

- Bridge priority
- Hello time
- Forwarding delay
- Maximum age time

This command can also disable STP and return the STP parameters to their default settings.

Note
You can use this command only if STP is designated as the active spanning tree protocol on the switch. See “ACTIVATE STP” on page 574.

Examples

The following command sets the switch's bridge priority value to 45,056 (increment 11):

```
set stp priority=11
```

The following command sets the hello time to 7 seconds and the forwarding delay to 25 seconds:

```
set stp hellotime=7 forwarddelay=25
```

The following command returns all STP parameters on the switch to the default values:

```
set stp default
```

Equivalent Command

```
purge stp
```

For information, see "PURGE STP" on page 577.

AlliedWare Plus Command

Syntax

```
spanning-tree priority priority
spanning-tree hello-time hello-time
spanning-tree forward-time forward-time
spanning-tree max-age max-age
```

Mode

Configure mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

The following commands set the hello time to 7 seconds and the forwarding delay to 25 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree hello-time 7
awplus(config)# spanning-tree forward-time 25
```

SET STP PORT

AlliedWare Plus
Command
Available

Syntax

```
set stp port=port [pathcost|portcost=auto|portcost]
[portpriority=portpriority]
```

Parameters

port
Specifies the port you want to configure. You can configure more than one port at a time. For instructions, refer to “Port Numbers in Commands” on page 48.

pathcost ***or*** portcost
Specifies the port’s cost. The parameters are equivalent. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost to the root bridge. This parameter can take the range of 1 to 65,535, or AUTO. The default setting is AUTO, for Automatic Update, which automatically sets port cost according to the speed of the port. Table 13 lists the STP port costs with Auto-Detect.

Table 13. STP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

Table 14 lists the STP port costs with Auto-Detect when a port is part of a port trunk.

Table 14. Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	4
100 Mbps	4
1000 Mbps	1

portpriority
Specifies the port’s priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16, for a total of 16 increments as shown in Table 15. You specify the increment of the desired value. The default is 128 (increment 8).

Table 15. Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

Description

This command is used to configure the following STP parameters settings for port:

- ❒ Port cost
- ❒ Port priority

Examples

The following command sets the port cost to 15 and the port priority to 192 (increment 12) for port 6:

```
set stp port=6 portcost=15 portpriority=12
```

The following command sets the port cost to auto-detect on ports 7 to 10:

```
set stp port=7-10 portcost=auto
```

AlliedWare Plus Command

Syntax

```
spanning-tree path-cost path-cost
spanning-tree priority priority
```

Mode

Port Interface mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

The following commands assign port 2 a port cost of 15 and a port priority of 192 (increment 12):

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2
awplus(config-if)# spanning-tree path-cost 15
awplus(config-if)# spanning-tree priority 12
```

SET SWITCH MULTICASTMODE

Syntax

```
set switch multicastmode=[a|b|c|d]
```

Parameter

multicast mode — Specifies the multicast mode. The options are:

- a Discards all the ingress spanning tree BPDU and 802.1x EAPOL packets.
- b Forwards the ingress spanning tree BPDU and 802.1x EAPOL packets across all the VLANs and the ports.
- c Forwards ingress BPDU and EAPOL packets only among the untagged ports of a VLAN where an ingress port is a member.
- d Forwards ingress BPDU and EAP packets on both the tagged and untagged ports of a VLAN where an ingress port is a member.

Description

This command controls the behavior of the switch or stack when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets when these features are disabled. Note the following when setting this parameter:

- This parameter is only adjustable with this command. It cannot be configured from the menus or web browser windows.
- The mode is set at the switch or stack level. It is not adjustable on a per-port basis.
- Only one mode can be active at a time.
- The mode setting applies to the spanning tree protocol BPDUs when STP, RSTP, and MSTP are disabled.
- The mode setting applies to the 802.1x port-based access control EAPOL packets when 802.1x is disabled.
- There are four possible states: A, B, C, and D:

A - Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all the ports. The switch or stack behaves as follows:

- If STP, RSTP, and MSTP are disabled, all the ingress BPDUs are discarded.

- ❐ If 802.1x port-based access control is disabled, all the ingress EAPOL packets are discarded.

B - Forwards the ingress spanning tree BPDU and 802.1x EAPOL packets across all the VLANs and the ports. The switch or stack behaves as follows:

- ❐ If STP, RSTP, and MSTP are disabled, the ingress BPDUs are flooded on all the ports.
- ❐ If STP, RSTP, MSTP, and 802.1x are disabled, the BPDU and EAPOL packets are flooded on all the ports.
- ❐ If STP or RSTP is enabled and 802.1x is disabled, the EAPOL packets are flooded on all the ports, except for ports in the blocking state.
- ❐ If MSTP is enabled and 802.1x is disabled, the EAPOL packets are flooded on all the ports, including ports in the blocking state.

C - Forwards the ingress BPDU and EAPOL packets only on untagged ports of the VLAN where the ingress port is a member. Packets are not forwarded from tagged ports. The VLAN is identified by the PVID assigned to the ingress port.

D - Forwards ingress BPDU and EAP packets from both tagged and untagged ports of the VLAN where the ingress port is a member. The VLAN is identified by the PVID assigned to the ingress port.

Example

This command sets the switch or stack mode to A to discard all ingress BPDUs and 802.1 EAPOL packets:

```
set switch multicastmode=a
```

SHOW STP

AlliedWare Plus
Command
Available

Syntax

```
show stp [port=port]
```

Parameter

port	Specifies the port whose STP parameters you want to view. You can view more than one port at a time.For instructions, refer to “Port Numbers in Commands” on page 48

Description

This command displays the current values for the STP parameters. An example of the display is shown in Figure 71.

```
Status ...................... Enabled
Bridge Priority ............. 32768 (In multiples of 4096: 8)
Bridge Hello Time ........... 2/2 (Configured/Actual)
Bridge Forwarding Delay ..... 15/15 (Configured/Actual)
Bridge Max Age .............. 20/20 (Configured/Actual)
Bridge Identifier ........... 32768/00:21:46:A7:B4:11
Root Bridge ................. 32768/00:21:46:A7:B4:11
Root Path Cost .............. 0
```

Figure 71. SHOW STP Command

The bridge priority, bridge hello time, and bridge max age parameters display two values when STP is enabled on the switch (for example, Bridge Forwarding Delay .. 15/15). The first number is the configured value on the switch for the parameter and the second is the value the switch obtained from the root bridge and is actually using for the parameter. The switch displays only the configured values when spanning tree is not activated on the switch.

The Status parameter displays whether STP is enabled or disabled on the switch.

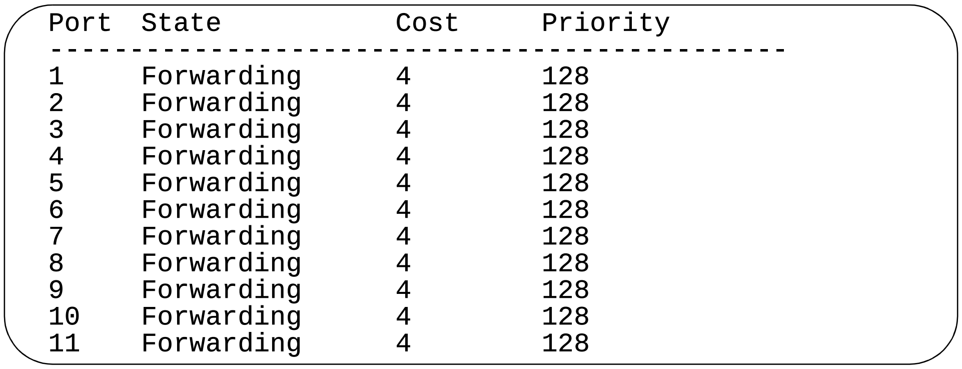
For definitions of the bridge priority, hello time, forwarding delay, and max age parameters, refer to “SET STP” on page 578.

The bridge Identifier parameter consists of the switch’s bridge priority value and MAC address, separated by a slash (/). To change the switch’s priority value, refer to “SET STP” on page 578. The MAC address of the switch cannot be changed.the MAC address of the switch.

The root bridge parameter specifies the bridge identifier of the root bridge of the spanning tree domain. The identifier consists of the bridge priority value and MAC address of the root switch, separated by a slash (/). This parameter only appears when STP is activated on the switch.

The root path cost parameter displays the path cost from the switch to the root bridge of the spanning tree domain. If the switch is the root bridge, the path cost is 0. This parameter only appears when STP is activated on the switch.

The PORT parameter allows you to view the STP parameter settings for the switch ports: An example of the display is shown in Figure 72.



```
Port  State           Cost     Priority
----------------------------------------------
1     Forwarding      4        128
2     Forwarding      4        128
3     Forwarding      4        128
4     Forwarding      4        128
5     Forwarding      4        128
6     Forwarding      4        128
7     Forwarding      4        128
8     Forwarding      4        128
9     Forwarding      4        128
10    Forwarding      4        128
11    Forwarding      4        128
```

Figure 72. SHOW STP PORT Command

Port is the port number.

State is the current state of a port. The possible states are Listening, Learning, Forwarding, or Blocking when spanning tree is enabled. When spanning tree is not enabled or if a port is not being used, its state will be disabled.

Cost is the port cost of the port.

Priority is the port's priority value. The number is used as a tie breaker when two or more ports have equal costs to the root bridge.

Examples

The following command displays the bridge STP settings:

```
show stp
```

The following command displays the STP settings for ports 1 to 4:

```
show stp port=1-4
```

AlliedWare Plus Command

Syntax

To display the bridge STP settings:

```
show spanning-tree detail
```

To display a port’s STP settings:

```
show spanning-tree interface port
```

Modes

User Exec mode and Privileged Exec mode

Description

These AlliedWare Plus commands are identical to the standard command.

Examples

This command displays the bridge STP settings:

```
awplus# show spanning-tree detail
```

This command displays the STP settings for ports 1 to 4:

```
awplus# show spanning-tree interface 1-4
```

Chapter 32

Rapid Spanning Tree Protocol (RSTP) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ACTIVATE RSTP

AlliedWare Plus
Command
Available

Syntax

```
activate rstp
```

Parameters

None.

Description

Use this command to designate RSTP as the active spanning tree. After you activate RSTP, you can enable or disable it using the ENABLE RSTP and DISABLE RSTP commands. RSTP is active on a switch or stack only after you have designated it as the active spanning tree with this command and enabled it with the ENABLE RSTP command.

Only one spanning tree protocol, STP, RSTP, or MSTP, can be active on the switch or stack at a time.

Example

The following command designates RSTP as the active spanning tree:

```
activate rstp
```

AlliedWare Plus Command

Syntax

```
spanning-tree mode rstp
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode rstp
```

DISABLE BPDUGUARD

AlliedWare Plus Command Available

Syntax

```
disable bpduguard
```

Parameters

None.

Description

This command is used to disable the BPDU guard feature. To view the current status of the feature, use "SHOW BPDUGUARD" on page 605.

Note
An edge port that is disabled by the BPDU guard feature remains in that state until you enable it with the management software. If a port is still receiving BPDUs, you will need to disconnect the network cable to prevent the feature from disabling it again.

Example

```
enable bpduguard
```

AlliedWare Plus Command

Syntax

```
no spanning-tree bpdu-guard
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree bpdu-guard
```

DISABLE RSTP

AlliedWare Plus Command Available

Syntax

```
disable rstp
```

Parameters

None.

Description

This command disables the Rapid Spanning Tree Protocol. To view the current status of RSTP, use “SHOW RSTP” on page 606.

Example

The following command disables RSTP:

```
disable rstp
```

AlliedWare Plus Command

Syntax

```
no spanning-tree rstp enable bridge-forward
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree rstp enable bridge-forward
```

ENABLE BPDUGUARD

AlliedWare Plus Command Available

Syntax

```
enable bpduguard
```

Parameters

None.

Description

This command is used to enable the BPDU guard feature, which monitors edge ports and disables them if they receive BPDU packets. To view the current status of this feature, use "SHOW BPDUGUARD" on page 605.

> **Note**
> An edge port that is disabled by the BPDU guard feature remains in that state until you enable it with the management software. If a port is still receiving BPDUs, you will need to disconnect the network cable to prevent the feature from disabling it again.

Example

```
enable bpduguard
```

AlliedWare Plus Command

Syntax

```
spanning-tree bpdu-guard
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree bpdu-guard
```

ENABLE RSTP

AlliedWare Plus
Command
Available

Syntax

```
enable rstp
```

Parameters

None.

Description

This command enables the Rapid Spanning Tree Protocol. To view the current status of RSTP, use “SHOW RSTP” on page 606. The default setting for RSTP is disabled.

You cannot enable RSTP until you have activated it with the ACTIVATE RSTP command.

Example

The following command enables RSTP:

```
enable rstp
```

AlliedWare Plus Command

Syntax

```
spanning-tree rstp enable
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree rstp enable
```

PURGE RSTP

Syntax

```
purge rstp
```

Parameters

None.

Description

This command returns all the RSTP bridge and port parameters to the default settings. RSTP must be disabled before you use this command. To disable RSTP, refer to "DISABLE RSTP" on page 592.

Example

The following command resets RSTP:

```
purge rstp
```

Equivalent Command

```
set rstp default
```

For information, refer to "SET RSTP" on page 596.

SET RSTP

AlliedWare Plus Command Available

Syntax

```
set rstp [default] [priority=priority] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
[rstptype|forceversion=stpcompatible|
forcestpcompatible|normalrstp]
```

Parameters

default
: Returns all bridge and port RSTP settings to the default values. This parameter cannot be used with any other command parameter and only when RSTP is disabled. (This parameter performs the same function as the PURGE RSTP command.)

priority
: Specifies the priority number for the bridge. This number is used in determining the root bridge for RSTP. The bridge with the lowest priority number is selected as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 16. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 16. Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

hellotime

Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

forwarddelay

Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The range is 4 to 30 seconds. The default is 15 seconds. This parameter effects only those ports operating in the STP compatible mode.

maxage

Specifies the length of time, in seconds, after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

Note
The value for the maxage parameter must be greater than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

rstptype ***or*** forceversion

Sets the RSTP mode. The parameters are equivalent. The options are:

stpcompatible ***or*** forcestpcompatible

The bridge uses the RSTP parameter settings, but transmits only STP BPDU packets from the ports. These options are equivalent.

normalrspt

The bridge uses RSTP. It transmits RSTP BPDU packets, except on ports connected to bridges running STP. This is the default setting.

Description

This command configures the following RSTP parameter settings.

- Bridge priority
- Hello time

❒ Forwarding delay

❒ Maximum age time

❒ Force version of STP or normal RSTP

This command can also return the RSTP parameters to their default settings.

Note
You can use this command only if RSTP is the active spanning tree protocol on the switch. See "ACTIVATE RSTP" on page 590.

Examples

The following command sets the bridge priority to 20480 (increment 5), the hello time to 5 seconds, and the forwarding delay to 20 seconds:

```
set rstp priority=5 hellotime=5 forwarddelay=20
```

The following command uses the FORCEVERSION parameter to configure the bridge to use the RSTP parameters but to transmit only STP BPDU packets:

```
set rstp forceversion=stpcompatible
```

The following command returns all RSTP parameter settings to their default values:

```
set rstp default
```

Equivalent Command

```
purge rstp
```

For information, see "PURGE RSTP" on page 595.

AlliedWare Plus Command

Syntax

```
spanning-tree priority priority
spanning-tree hello-time hello-time
spanning-tree forward-time forward-time
spanning-tree max-age max-age
spanning-tree forceversion 1|2|3
```

Mode

Configure mode

Description

These AlliedWare Plus commands are identical to the standard command.

Examples

The following commands set the hello time to 7 seconds and the forwarding delay to 25 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree hello-time 7
awplus(config)# spanning-tree forward-time 25
```

The FORCEVERSION parameter sets the RSTP mode. Settings 1 and 2 are STP compatible and force STP compatible, respectively. These settings are identical. Setting 3 is normal RSTP. These commands set the switch to STP compatible:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forceversion 1
```

SET RSTP PORT

AlliedWare Plus Command Available

Syntax

```
set rstp port=port [pathcost|portcost=cost|auto]
[portpriority=portpriority]
[edgeport=yes|no|on|off|true|false]
[ptp|pointtopoint=yes|no|on|off|true|false|autoupdate]
[migrationcheck=yes|no|on|off|true|false]
[loopguard=enabled|disabled]
```

Parameters

port — Specifies the port you want to configure. You can specify more than one port at a time. For instructions, refer to “Port Numbers in Commands” on page 48.

pathcost ***or*** portcost — Specifies the port’s cost. The parameters are equivalent. The spanning tree algorithm uses the cost parameter to decide which port provides the lowest cost path to the root bridge for that LAN. The options are:

cost — A number for the port cost. The range is 1to 200,000,000.

auto — Automatically sets the port cost according to the speed of the port. This is the default. Table 17 lists the port cost with auto-detect.

Table 17. RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 18 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 18. RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000

Table 18. RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
1000 Mbps	2,000

portpriority — Specifies the port's priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16, for a total of 16 increments, as shown in Table 19. You specify the increment that corresponds to the desired value. The default is 128, which is increment 8.

Table 19. Port Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

edgeport — Defines whether the port is functioning as an edge port. An edge port is connected to a device operating at half-duplex mode and is not connected to any device running STP or RSTP. The options are:

yes, on, true	The port is an edge port. The options are equivalent.
no, off, false	The port is not an edge port. The options are equivalent. This is the default.

ptp ***or*** pointtopoint — Defines whether the port is functioning as a point-to-point port. The parameters are equivalent. This type of port is connected to a device operating at full-duplex mode. The options are:

yes, on, true	The port is an point-to-point port. The options are equivalent.

no, off, false — The port is not an point-to-point port. The parameters are equivalent. are equivalent.

autoupdate — The port’s status is determined automatically. This is the default.

migrationcheck — Enables and disables migration check. The purpose of this feature is to change from the RSTP mode to the STP mode if STP BDPU packets are received on the selected port. When you enable this option, the bridge will send out RSTP BPDU packets from the selected port until STP BPDU packets are received. The port will remain in the RSTP mode until it receives an STP BPDU packet. The options are:

yes, on, true — Enable migration check. The options are equivalent.

no, off, false — Disable migration check. The options are equivalent.

loopguard — Enables and disables the loop guard feature on a port. This features disables a port if it stops receiving BPDUs when there is no change to the link status.

Description

This command sets a port’s RSTP settings.

Examples

The following command sets the port cost to 1,000,000 and port priority to 224 (increment 14) on port 4:

```
set rstp port=4 portcost=1000000 portpriority=14
```

The following command changes ports 6 to 8 so they are not considered edge ports:

```
set rstp port=6-8 edgeport=no
```

AlliedWare Plus Command

Syntax

```
spanning-tree path-cost path-cost
spanning-tree priority priority
spanning-tree edgeport|portfast
spanning-tree link-type point-to-point|shared
spanning-tree loop-guard
no spanning-tree loop-guard
```

Note
The EDGEPORT and PORTFAST parameters are equivalent.

Mode

Port Interface mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

The following commands assign port 2 a port cost of 15 and a port priority of 192 (increment 12):

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2
awplus(config-if)# spanning-tree path-cost 15
awplus(config-if)# spanning-tree priority 12
```

The following commands designate port 22 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22
awplus(config-if)# spanning-tree edgeport
```

The following commands designate ports 17 and 23 as not edge ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 17,23
awplus(config-if)# no spanning-tree edgeport
```

This example designates ports 11 to 23 as point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11-23
awplus(config-if)# spanning-tree link-type point-to-point
```

This example designates ports 26 and 27 as not point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 26,27
awplus(config-if)# spanning-tree link-type shared
```

This example activates the loop guard feature on ports 5 and11:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5,11
awplus(config-if)# spanning-tree loop-guard
```

SHOW BPDUGUARD

Syntax

```
show bpduguard
```

Parameters

None.

Description

This command displays the status of BPDU guard on the switch. The status can be either enabled or disabled.

Example

This command displays the status of BPDU guard.

```
show bpduguard
```

SHOW RSTP

AlliedWare Plus
Command
Available

Syntax

`show rstp [portconfig=`*`port`*`] [portstate=`*`port`*`]`

Parameters

portconfig Displays the RSTP port settings. You can specify more than one port at a time. For instructions, refer to “Port Numbers in Commands” on page 48.

portstate Displays the RSTP status of the ports. You can specify more than one port at a time.

Description

You use this command to display the RSTP parameter settings. Entering the command without either of the parameters displays the information shown in Figure 73.

```
Status ...................... Enabled
Force Version ............... NormalRSTP
Bridge Priority ............. 32768 (In multiples of 4096: 8)
Bridge Hello Time ........... 2/2 (Configured/Actual)
Bridge Forward Delay ........ 15/15 (Configured/Actual)
Bridge Max Age .............. 20/20 (Configured/Actual)
Bridge Identifier ........... 32768/00:21:46:A7:B4:11
Root Bridge Identifier ...... 32768/00:21:46:A7:B4:11
Root Path Cost .............. 0
```

Figure 73. Example of the SHOW RSTP Command

The bridge priority, bridge hello time, and bridge max age parameters will have two values if RSTP is enabled on the switch (for example, Bridge Forwarding .. 15/15). The first number is the configured value on the switch for the parameter and the second is the value the switch obtained from the root bridge and is currently using for the parameter. The switch displays only the configured values for these parameters if spanning tree is not enabled on the switch.

The Status parameter indicates whether STP is enabled or disabled.

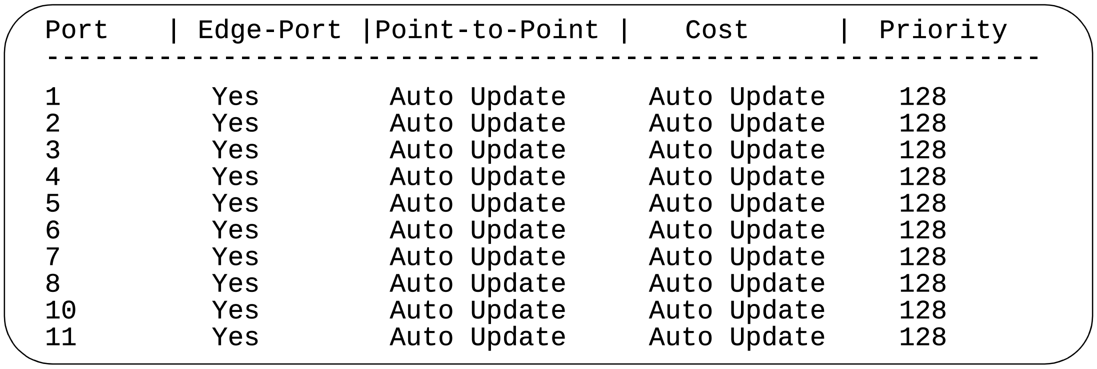
For definitions of the force version, bridge priority, hello time, forward delay, and max age parameters, refer to “SET RSTP” on page 596.

The bridge Identifier parameter consists of the switch’s bridge priority value and MAC address, separated by a slash (/). To change the switch’s priority value, refer to “SET RSTP” on page 596. The MAC address of the switch cannot be changed.

The root bridge identifier parameter displays the bridge priority value and MAC address of the root switch of the spanning tree domain. The values are separated by a slash (/). This parameter only appears when RSTP is activated on the switch.

The root path cost parameter displays the path cost from the switch to the root bridge of the spanning tree domain. If the switch is the root bridge, the path cost is 0. This parameter only appears when RSTP is activated on the switch.

The PORTCONFIG parameter displays the current RSTP parameter settings for the ports. An example is shown in Figure 74.

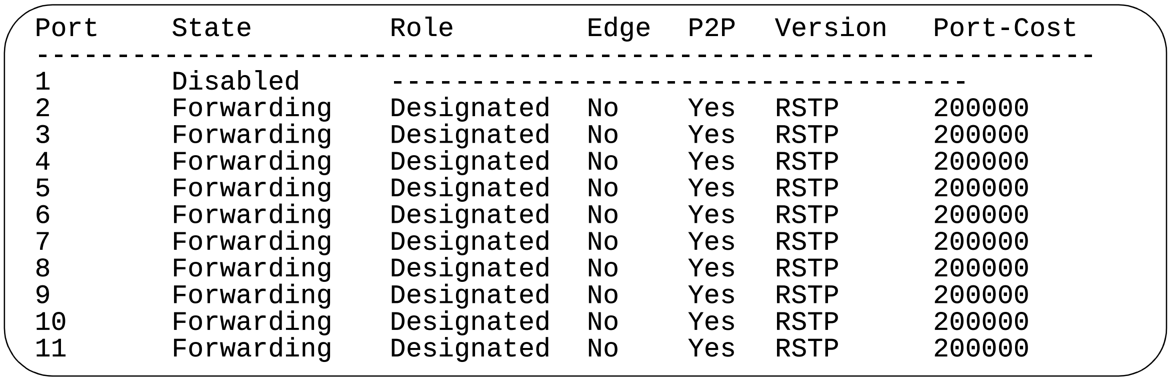


```
Port    | Edge-Port |Point-to-Point |    Cost     |  Priority
---------------------------------------------------------------

1         Yes        Auto Update     Auto Update    128
2         Yes        Auto Update     Auto Update    128
3         Yes        Auto Update     Auto Update    128
4         Yes        Auto Update     Auto Update    128
5         Yes        Auto Update     Auto Update    128
6         Yes        Auto Update     Auto Update    128
7         Yes        Auto Update     Auto Update    128
8         Yes        Auto Update     Auto Update    128
10        Yes        Auto Update     Auto Update    128
11        Yes        Auto Update     Auto Update    128
```

Figure 74. Example of the SHOW RSTP PORTCONFIG Command

For definitions of these parameters, refer to "SET RSTP PORT" on page 600.

The PORTSTATE parameter displays the current operating settings and status of the ports. An example is shown in Figure 75.



```
Port     State        Role        Edge  P2P  Version   Port-Cost
------------------------------------------------------------------
1        Disabled     ------------------------------------
2        Forwarding   Designated  No    Yes  RSTP      200000
3        Forwarding   Designated  No    Yes  RSTP      200000
4        Forwarding   Designated  No    Yes  RSTP      200000
5        Forwarding   Designated  No    Yes  RSTP      200000
6        Forwarding   Designated  No    Yes  RSTP      200000
7        Forwarding   Designated  No    Yes  RSTP      200000
8        Forwarding   Designated  No    Yes  RSTP      200000
9        Forwarding   Designated  No    Yes  RSTP      200000
10       Forwarding   Designated  No    Yes  RSTP      200000
11       Forwarding   Designated  No    Yes  RSTP      200000
```

Figure 75. Example of the SHOW RSTP PORTSTATE Command

The information displayed by the command is as follows:

- Port — The port number.
- State — The RSTP state of the port. The possible states for a port connected to another device running RSTP are Discarding and Forwarding.

  The possible states for a port connected to a device running STP are Listening, Learning, Forwarding, and Blocking.

  The possible states for a port not being used or where spanning tree is not activated is Disabled.
- Role — The RSTP role of the port. Possible roles are:

  Root - The port is connected to the root switch, directly or through other switches, with the least path cost.

  Alternate - The port offers an alternate path to the root switch.

  Backup - The port on a designated switch that provides a backup for the path provided by the designated port.

  Designated - The port has the least cost path to the root switch.
- P2P — Whether or not the port is functioning as a point-to-point port. The possible settings are Yes and No.
- Version — Whether the port is operating in RSTP mode or STP-compatible mode.
- Port Cost — The current operating cost of the port.

Examples

The following command displays the bridge’s RSTP settings:

```
show rstp
```

The following command displays the RSTP port settings for ports 1 to 4:

```
show rstp portconfig=1-4
```

The following command displays RSTP port status for port 15:

```
show rstp portstate=15
```

AlliedWare Plus Command

Syntax

To display the bridge RSTP settings:

```
show spanning-tree detail
```

To display the RSTP status of the ports:

```
show spanning-tree interface port
```

Mode

User Exec mode and Privileged Exec mode

Description

The first command is equivalent to the SHOW RSTP command without either of the parameters. The second command is equivalent to the PORTSTATE parameter. There is no equivalent AlliedWare Plus command for the PORTCONFIG parameter.

Examples

This command displays the bridge RSTP settings:

```
awplus# show spanning-tree detail
```

This command displays the RSTP states for ports 1 to 4:

```
awplus# show spanning-tree interface 1-4
```

Chapter 33

Multiple Spanning Tree Protocol (MSTP) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

ACTIVATE MSTP

AlliedWare Plus Command Available

Syntax

```
activate mstp
```

Parameters

None.

Description

This command designates MSTP as the active spanning tree on the switch. You cannot enable MSTP or configure its parameters until after you have designated it as the active spanning tree with this command.

Only one spanning tree protocol can be active on the switch at a time.

Example

The following command designates MSTP as the active spanning tree:

```
activate mstp
```

AlliedWare Plus Command

Syntax

```
spanning-tree mode mstp
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mode mstp
```

ADD MSTP

Syntax

```
add mstp mstiid=mstiid mstivlanassoc=vids
```

Parameters

mstiid
Specifies the ID of the multiple spanning tree instance (MSTI) to which you want to associate VLANs. You can specify only one MSTI ID at a time. The range is 1 to 15.

mstivlanassoc
Specifies the VID of the VLAN you want to associate with the MSTI ID. You can specify more than one VID at a time (for example, 2,5,44).

Description

This command associates VLANs to MSTIs.

The MSTIID parameter specifies the MSTI ID. The MSTI must already exist on the switch. To create a spanning tree instance, see “CREATE MSTP” on page 614.

The MSTIVLANASSOC parameter specifies the VIDs of the VLANs you want to associate with the MSTI. The VLANs must already exist on the switch. Any VLANs already associated with the MSTI are retained. If you want to add VLANs to a MSTI while removing those already associated to it, see “SET MSTP MSTIVLANASSOC” on page 628.

Examples

The following command associates the VLAN with the VID 4 to MSTI ID 8:

```
add mstp mstiid=8 mstivlanassoc=4
```

The following command associates the VLANs with the VIDs 24 and 44 to MSTI ID 11:

```
add mstp mstiid=11 mstivlanassoc=24,44
```

CREATE MSTP

AlliedWare Plus Command Available

Syntax

```
create mstp mstiid=mstiid [mstivlanassoc=vids]
```

Parameters

mstiid — Specifies the MSTI ID of the spanning tree instance you want to create. You can specify only one MSTI ID at a time. The range is 1 to 15.

mstivlanassoc — Specifies the VID of the VLAN you want to associate with the MSTI ID. You can specify more than one VID at a time (for example, 2,5,44).

Description

This command is used to create new multiple spanning tree instances and to associate VLANs to the instances.

The MSTIID parameter specifies the ID number for the new spanning tree instance.

The MSTIVLANASSOC parameter specifies the VIDs of the VLANs you want to associate with the new MSTI. The VLANs must already exist on the switch. If you do not specify any VLANs, you can add them later using “ADD MSTP” on page 613 or “SET MSTP MSTIVLANASSOC” on page 628.

Examples

The following command creates the MSTI ID 8 and associates to it the VLAN with the VID 4:

```
create mstp mstiid=8 mstivlanassoc=4
```

The following command creates the MSTI ID 11 and associates to it the VLANs with the VIDs 24 and 44:

```
create mstp mstiid=11 mstivlanassoc=24,44
```

AlliedWare Plus Command

Syntax

```
instance mstiid vids [priority]
```

Mode

Multiple spanning tree mode

Description

This AlliedWare Plus command has the following rules and restrictions:

- This command differs from the CREATE MSTP MSTIID command in that it allows you to assign a priority number to a new MSTI. The priority number is applied to all of the ports that are members of the associated VLANs. You can specify only one priority number. For the priority values, refer to "SET MSTP PORT" on page 629. This parameter is optional.
- The VLAN associations are required with this command. They are optional with the CREATE MSTP command.

Example

These commands create a new multiple spanning tree instance that has the ID 5. There are two VLANs associated with the instance. The VIDs are 11 and 21. The priority value of the MTSI is 64 (increment 4):

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# instance 5 11,21 4
```

DELETE MSTP

Syntax

```
delete mstp mstiid=mstiid mstivlanassoc=vids
```

Parameters

mstiid	Specifies the MSTI ID of the spanning tree instance where you want to remove VLANs. You can specify only one MSTI ID at a time. The range is 1 to 15.
mstivlanassoc	Specifies the VID of the VLAN you want to remove from the spanning tree instance. You can specify more than one VID at a time (for example, 2,5,44).

Description

This command removes VLANs from spanning tree instances and returns them to CIST.

The MSTIID parameter specifies the MSTI ID.

The MSTIVLANASSOC parameter specifies the VIDs of the VLANs you want to remove from the spanning tree instance.

Examples

The following command deletes the VLAN with the VID 4 from MSTI ID 8:

```
delete mstp mstiid=8 mstivlanassoc=4
```

The following command deletes the VLANs with the VIDs 24 and 44 from MSTI ID 11:

```
delete mstp mstiid=11 mstivlanassoc=24,44
```

DESTROY MSTP MSTIID

AlliedWare Plus
Command
Available

Syntax

```
destroy mstp mstiid=mstiid
```

Parameter

mstiid	Specifies the MSTI ID of the spanning tree instance you want to delete. You can specify only one MSTI ID at a time. The range is 1 to 15.

Description

This command deletes multiple spanning tree instances and returns the VLANs of the deleted MSTIs to CIST.

Example

The following command deletes the spanning tree instance 4:

```
destroy mstp mstiid=4
```

AlliedWare Plus Command

Syntax

```
no instance mstiid
```

Mode

Multiple spanning tree mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

These commands delete MSTI 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# no instance 4
```

DISABLE MSTP

AlliedWare Plus Command Available

Syntax

```
disable mstp
```

Parameters

None.

Description

This command disables the Multiple Spanning Tree Protocol on the switch. To view the current status of MSTP, refer to “SHOW MSTP” on page 635.

Example

The following command disables MSTP:

```
disable mstp
```

AlliedWare Plus Command

Syntax

```
no spanning-tree mstp enable bridge-forward
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no spanning-tree mstp enable bridge-forward
```

ENABLE MSTP

AlliedWare Plus Command Available

Syntax

```
enable mstp
```

Parameters

None.

Description

This command enables Multiple Spanning Tree Protocol on the switch or stack. To view the current status of MSTP, refer to "SHOW MSTP" on page 635.

You must select MSTP as the active spanning tree on the switch before you can enable it with this command. To activate MSTP, see "ACTIVATE MSTP" on page 612.

Example

The following command enables MSTP:

```
enable mstp
```

AlliedWare Plus Command

Syntax

```
spanning-tree mstp enable
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mstp enable
```

PURGE MSTP

Syntax

```
purge mstp
```

Parameters

None.

This command returns all the MSTP bridge and port parameters settings to their default values. This command also deletes all multiple spanning tree instances and VLAN associations.

In order for you to use this command, MSTP must be the active spanning tree protocol on the switch and the protocol must be disabled. To select MSTP as the active spanning tree protocol on the switch, see “ACTIVATE MSTP” on page 612. To disable MSTP, refer to “DISABLE MSTP” on page 618.

Example

The following command resets the MSTP bridge and port parameter settings:

```
purge mstp
```

Equivalent Command

```
set mstp default
```

For information, see “SET MSTP” on page 621.

SET MSTP

AlliedWare Plus Command Available

Syntax

```
set mstp [default]
[forceversion=stpcompatible|forcestpcompatible|
normalmstp] [hellotime=hellotime]
[forwarddelay=forwarddelay] [maxage=maxage]
[maxhops=maxhops] [configname="name"]
[revisionlevel=number]
```

Parameters

default

Disables MSTP and returns all bridge and port MSTP settings to the default values. This parameter cannot be used with any other parameter. (This parameter performs the same function as the PURGE MSTP command.) The spanning tree protocol must be disabled to use this parameter.

forceversion

Controls whether the bridge will operate with MSTP or in an STP-compatible mode. If you select MSTP, the bridge will operate all ports in MSTP, except for those ports that receive STP or RSTP BPDU packets. If you select STP Compatible or Force STP Compatible, the bridge uses its MSTP parameter settings, but sends only STP BPDU packets from the ports

The options are:

normalmspt

The bridge uses MSTP. The bridge sends out MSTP BPDU packets from all ports except for those ports connected to bridges running STP. This is the default setting.

stpcompatible ***or*** forcestpcompatible

The bridge operates in an STP-compatible mode where it uses the MSTP parameter settings, but transmits only STP BPDU packets from the ports. These options are equivalent.

Note

Selecting the STP-compatible mode deletes all spanning tree instances on the switch.

---

hellotime

Specifies the time interval between generating and sending configuration messages by the bridge. This parameter can be from 1 to 10 seconds. The default is 2 seconds.

forwarddelay

Specifies the waiting period before a bridge changes to a new state, for example, becomes the new root bridge after the topology changes. If the bridge transitions too soon, not all links may have yet adapted to the change, resulting in network loops. The default is 15 seconds. This parameter effects only those ports operating in the STP compatible mode.

maxage

Specifies the length of time, in seconds, after which stored bridge protocol data units (BPDUs) are deleted by the bridge. All bridges in a bridged LAN use this aging time to test the age of stored configuration messages called bridge protocol data units (BPDUs). For example, if you use the default value of 20, all bridges delete current configuration messages after 20 seconds. The range of this parameter is 6 to 40 seconds. The default is 20 seconds.

Note

The value for the maxage parameter must be greater than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

maxhops

Specifies the maximum hops counter. MSTP regions use this parameter to discard BPDUs. The Max Hop counter in a BPDU is decremented every time the BPDU crosses a bridge within a MSTP region. After the counter reaches zero, the BPDU is deleted. The counter is reset to its original value if the BPDU crosses a MSTP regional boundary.

configname

Specifies the name of the MSTP region. The range is 0 (zero) to 32 alphanumeric characters. The name is case-sensitive and must be the same on all bridges in a region. Examples include Sales Region and Production Region. The name must be enclosed in quotes.

revisionlevel

Specifies the revision number of an MSTP region. The range is 0 (zero) to 255. This is an arbitrary number that you assign to a region. The reversion level must be the same on all the bridges in a region. Different regions can have the same reversion level without conflict.

Description

This command configures the following MSTP parameter settings.

- ❐ Hello time
- ❐ Forwarding delay
- ❐ Maximum age time
- ❐ Maximum hop count
- ❐ Force version of STP or normal MSTP
- ❐ Configuration name
- ❐ Revision level

Examples

The following command disables MSTP and returns all MSTP parameter settings to their default values:

```
set mstp default
```

The following command sets the hop count to 10, the configuration name to Engineering Region, and the reversion level to 2:

```
set mstp maxhops=10 configname="Engineering Region"
revisionlevel=2
```

The following command uses the FORCEVERSION parameter to configure the bridge to use the MSTP parameters but to transmit only STP BPDU packets:

```
set mstp forceversion=forcestpcompatible
```

Equivalent Command

```
purge mstp
```

For information, see “PURGE MSTP” on page 620. This command performs the same function as the DEFAULT parameter.

AlliedWare Plus Command

Syntax

To specify whether the bridge will operate with MSTP or in an STP-compatible mode

```
forceversion 1|2|3
```

To specify the revision number of an MSTP region:

```
revision revisionlevel
```

To set a region’s name:

```
region configname
```

Mode

For he FORCEVERSION command:

Configure mode

For the REVISION and REGION commands:

Multiple spanning tree mode

Description

The AlliedWare Plus commands let you change only the MSTP parameters listed above. To change the other parameters, use the standard command or another management interface.

Example

This example sets the region’s revision level to 10 and its name to ‘sw10a:’

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# revision 10
awplus(config-mst)# region sw10a
```

The FORCEVERSION command sets the MSTP mode. Settings 1 and 2 are STP compatible and force STP compatible, respectively. These settings are identical. Setting 3 is normal MSTP. These commands set the switch to STP compatible:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree forceversion 1
```

SET MSTP CIST

Syntax

```
set mstp cist priority=priority
```

Parameter

priority Specifies the CIST priority number for the switch. The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 20. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 20. CIST Priority Value Increments

Increment	CIST Priority	Increment	CIST Priority
0	0	8	32768
1	4096	9	36864
2	8192	10	40960
3	12288	11	45056
4	16384	12	49152
5	20480	13	53248
6	24576	14	57344
7	28672	15	61440

Description

This command sets the CIST priority number on the switch. This number is used to determine the root bridge for the bridged network. The bridge with the lowest priority number acts as the root bridge. If two or more bridges have the same priority value, the bridge with the numerically lowest MAC address becomes the root bridge. To view the current CIST priority number, see “SHOW MSTP” on page 635.

Example

The following command sets the CIST priority value to 45,056, which is increment 11:

```
set mstp cist priority=11
```

SET MSTP MSTI

Syntax

```
set mstp msti mstiid=mstiid priority=priority
```

Parameters

mstiid Specifies a MSTI ID. You can specify only one MSTI ID at a time. The range is 1 to 15.

priority Specifies the MSTI priority value for the switch. The range is 0 to 61,440 in increments of 4,096. The range is divided into sixteen increments, as shown in Table 21. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 21. MSTI Priority Value Increments

Increment	MSTI Priority	Increment	MSTI Priority
0	0	8	32,768
1	4,096	9	36,864
2	8,192	10	40,960
3	12,288	11	45,056
4	16,384	12	49,152
5	20,480	13	53,248
6	24,576	14	57,344
7	28,672	15	61,440

Description

This command changes the MSTI priority value of a spanning tree instance on a bridge. This value is used in determining the regional root bridge of a spanning tree instance.

The MSTIID parameter specifies the MSTI ID whose MSTI priority you want to change. The range is 1 to 15.

The PRIORITY parameter specifies the new MSTI priority value. The range is 0 (zero) to 61,440 in increments of 4,096, with 0 being the highest priority.

Examples

The following command changes the MSTI priority value to 45,056 (increment 11) for the MSTI ID 4:

```
set mstp msti mstiid=4 priority=11
```

The following command changes the MSTI priority value to 8,192 (increment 2) for the MSTI ID 6:

```
set mstp msti mstiid=6 priority=2
```

SET MSTP MSTIVLANASSOC

Syntax

```
set mstp mstivlanassoc mstiid=mstiid vlanlist=vids
```

Parameters

mstiid — Specifies the ID of the spanning tree instance where you want to associate VLANs. You can specify only one MSTI ID at a time. The range is 1 to 15.

vlanlist — Specifies the VID of the VLAN you want to associate with the MSTI ID. You can specify more than one VID at a time (for example, 2,5,44). If VLANs have already been associated with the MSTI, they are overwritten.

Description

This command associates VLANs to spanning tree instances.

The MSTIID parameter specifies the ID of the spanning tree instance. The spanning tree instance must already exist on the switch. To create a spanning tree instance, see “CREATE MSTP” on page 614.

The VLANLIST parameter specifies the VID of the VLANs you want to associate with the MSTI. The VLANs must already exist on the switch. If VLANs are already associated with the MSTI, they are removed and returned to CIST. If you want to add VLANs to an MSTI and retain those VLANs already associated with it, see “ADD MSTP” on page 613.

Examples

The following command associates the VLAN with the VID 4 to MSTI ID 8:

```
set mstp mstivlanassoc mstiid=8 vlanlist=4
```

The following command associates VIDs 24 and 44 to MSTI ID 11:

```
set mstp mstivlanassoc mstiid=11 vlanlist=24,44
```

SET MSTP PORT

AlliedWare Plus
Command
Available

Syntax 1

```
set mstp port=port|all [extportcost=auto|portcost]
[edgeport=yes|no|no|on|off|true|false]
[ptp|pointtopoint=yes|no|on|off|true|false|autoupdate]
[migrationcheck=yes|no|on|off|true|false]
```

Syntax 2

```
set mstp port=port|all [intportcost=auto|portcost]
[portpriority=priority] [stpid=msti_id]
```

Parameters

port
Specifies the port you want to configure. You can specify more than one port at a time. For instructions, refer to "Port Numbers in Commands" on page 48. To configure all the ports in the switch, enter ALL.

extportcost
Specifies the cost of a port connected to a bridge that is a member of another MSTP region or is running STP or RSTP. This is referred to as an external port cost. The range is 0 to 200,000,000. The default setting is Auto, which sets port cost based on port speed. Table 22 lists the MSTP external port costs with the Auto setting when the port is not a member of a trunk.

Table 22. Auto External Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 23 lists the MSTP port costs with the Auto setting when the port is part of a port trunk.

Table 23. Auto External Path Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
1000 Mbps	2,000

edgeport

Defines whether the port is functioning as an edge port. An edge port is connected to a device operating at half-duplex mode and is not connected to any device running STP or MSTP. Selections are:

yes, on, true	The port is an edge port. These values are equivalent. This is the default.
no, off, false	The port is not an edge port. These values are equivalent.

ptp ***or*** pointtopoint

Defines whether the port is functioning as a point-to-point port. This type of port is connected to a device operating at full-duplex mode. Selections are:

yes, on, true	The port is an point-to-point port.
no, off, false	The port is not an point-to-point port.
autoupdate	The port's status is determined automatically. This is the default.

migrationcheck

This parameter resets a MSTP port, allowing it to send MSTP BPDUs. When a MSTP bridge receives STP BPDUs on an MSTP port, the port transmits STP BPDUs. The MSTP port continues to transmit STP BPDUs indefinitely. Set the migrationcheck parameter to yes to reset the MSTP port to transmit MSTP BPDUs.

yes, on, true	Enable migration check. The values are equivalent.
no, off, false	Disable migration check. The values are equivalent.

Note

Each time a MSTP port is reset by STP BPDUs, set the migrationcheck parameter to yes, allowing the port to send MSTP BPDUs.

intportcost

Specifies the cost of a port connected to a bridge that is part of the same MSTP region. This is referred to as an internal port cost. The range is 0 to 200,000,000. The default setting is Auto-detect (0), which sets port cost depending on the speed of the port. Default values are 2,000,000 for 10 Mbps ports, 200,000 for a 100 Mbps ports, and 20,000 for one gigabit ports.

portpriority Specifies the port's priority. This parameter is used as a tie breaker when two or more ports are determined to have equal costs to the root bridge. The range is 0 to 240 in increments of 16. There are sixteen increments, as shown in Table 24 on page 631. You specify the increment of the desired value. The default is 128, which is increment 8.

Table 24. Port Priority Value Increments

Increment	Port Priority	Increment	Port Priority
0	0	8	128
1	16	9	144
2	32	10	160
3	48	11	176
4	64	12	192
5	80	13	208
6	96	14	224
7	112	15	240

stpid Specifies the ID number of an MSTI in which the VLAN of a port is a member. This parameter is used with the INTPORTCOST and PORTPRIORITY parameters to assign different path costs and priority values to untagged and tagged ports whose VLANs belong to more than one MSTI. You can specify more than one MSTI at a time (e.g., 4,6,11). If the VLANs of a port belong to just one MSTI, you can omit this parameter.

Description

This command sets a port's MSTP settings. The command is illustrated in two syntaxes to represent the two groups of MSTI port parameters. The first group is referred to as generic parameters. They are set just once on a port, regardless of the number of MSTIs where a port is a member. These parameters are the external path cost and edge port and point-to-point port designations.

The second group can be applied independently on a port on a per-MSTI basis. There are two parameters in this group — internal path cost and priority. A port whose VLANs are members of different MSTIs can have different settings in each MSTI. The MSTI is identified with the STPID parameter. You can omit the STPID parameter if a port is a member of one or more VLANs that all belong to the same MSTI, or if you want to assign the port the same path cost or priority value in all of its MSTI assignments.

Synax 1 Examples

The following command sets the external port cost to 500 for Ports 14 and 23:

```
set mstp port=14,23 extportcost=500
```

The following command sets the external port cost to 1,000,000 for Port 4 and designates it as an edge port:

```
set mstp port=6-8 edgeport=yes
```

The following command sets the external port cost for Ports 2 and 5 to Auto, which sets the port cost based on speed:

```
set mstp port=2-5 extportcost=auto
```

The following command designates Ports 6 to 8 as point-to-point ports:

```
set mstp port=6-8 ptp=yes
```

Syntax 2 Examples

The following command sets the internal port cost to 500 for Ports 7 and 10. If the ports are members of more than one VLAN and the VLANs are assigned to more than one MSTI, the new internal port cost is assigned to all of their MSTI assignments:

```
set mstp port=7,10 intportcost=500
```

This example illustrates the STPID parameter. This parameter is used when a port belongs to more than one VLAN and the VLANs are assigned to different MSTIs. You can use the parameter to specify different priority and internal port costs on a port for each MSTI assignment. This command assigns Port 15 in MSTI 2 a priority of 64 (increment 4):

```
set mstp port=7,10 portpriority=4 stpid=2
```

The following command sets the internal port cost to 1,000,000 and port priority to 224 (increment 14) for Port 4:

```
set mstp port=4 intportcost=1000000 portpriority=14
```

The following command is similar to the previous example, except it assumes port 4 is a member of more than one MSTI and you want to assign the new values to only one of its MSTI assignments, in this case MSTI 12:

```
set mstp port=4 intportcost=1000000 portpriority=14 stpid=12
```

The following command sets the internal port cost for Ports 2 and 5 to Auto, which sets the port cost based on speed:

```
set mstp port=2-5 intportcost=auto
```

AlliedWare Plus Command

Syntax

```
spanning-tree path-cost path-cost
spanning-tree priority priority
spanning-tree edgeport|portfast
spanning-tree link-type point-to-point|shared
```

Mode

Port Interface mode

Description

This AlliedWare Plus command has the following rules and restrictions:

- The PATH-COST parameter sets the external path cost of a port.
- The EDGEPORT and PORTFAST parameters are equivalent and are used to specify whether or not a port is an edge port of an MSTI.
- You cannot use the AlliedWare Plus commands to set the internal port cost or the migration check of a port. To set these parameters, use the standard command or another management interface.
- When setting a port's priority, you can use the SPANNING TREE PRIORITY command in the Port Interface mode if the port has just one MSTI or if it has multiple MSTIs and you want to assign all of them the same priority value. However, if you want to assign different priority values to a port that belongs to more than one MSTI, use the standard command.

Examples

These commands assign port 2 a port cost of 15 and a port priority of 192 (increment 12):

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2
awplus(config-if)# spanning-tree path-cost 15
awplus(config-if)# spanning-tree priority 12
```

These commands designate port 22 as an edge port:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22
awplus(config-if)# spanning-tree edgeport
```

These commands designate ports 17 and 23 as not edge ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 17,23
awplus(config-if)# no spanning-tree edgeport
```

These commands designate ports 11 to 23 as point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 11-23
awplus(config-if)# spanning-tree link-type point-to-point
```

These commands designate ports 26 and 27 as not point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 26,27
awplus(config-if)# spanning-tree link-type shared
```

These commands designate ports 26 and 27 as not point-to-point ports:

```
awplus> enable
awplus# configure terminal
awplus(config)# spanning-tree mst configuration
awplus(config-mst)# spanning-tree link-type shared
```

SHOW MSTP

AlliedWare Plus Command Available

Syntax

```
show mstp [portconfig=ports] [portstate=ports]
[stpid=msti_id] [mstistate] [cist] [mstivlanassoc]
```

Parameters

portconfig Displays the MSTP settings of a port. You can specify more than one port at a time. For a list of the MSTP information displayed by this parameter, refer to the Description below.

portstate Displays the MSTP state of a port. You can specify more than one port at a time. For a list of the MSTP information displayed by this parameter, refer to Description below.

stpid Specifies an MSTI ID. This parameter is used with the PORTCONFIG and PORTSTATE parameters to view the MSTP settings of ports that belong to VLANs that are members of different MSTIs. You can specify more than one MSTI ID.

mstistate Displays a list of the MSTIs on the switch and their associated VLANs. The list does not include the CIST.

cist Displays the CIST priority and the VLANs associated with CIST.

mstivlanassoc Displays a list of the MSTIs on the switch, including the CIST, and their associated VLANs.

Note
You can specify only one parameter at a time in this command. The only exception is the STPID parameter, which is used with the PORTCONFIG and PORTSTATE parameters.

Description

This command displays MSTP parameters. Entering SHOW MSTP without any parameters displays the following MSTP settings:

- MSTP status
- Force version
- Hello time

- Forwarding delay
- Maximum age
- Maximum hops
- Configuration name
- Reversion level
- Bridge identifier
- Root identifier

The hello time, forwarding delay, and bridge max age parameters will have two values if MSTP is enabled on the switch (for example, Forwarding Delay .. 15/15). The first number is the configured value on the switch for the parameter and the second is the value the switch obtained from the root bridge and is actually using for the parameter. The switch displays only the configured values for these parameters if spanning tree is not enabled on the switch.

The bridge Identifier parameter consists of the switch's CIST priority value and MAC address, separated by a slash (/). To change the CIST priority value, refer to "SET MSTP CIST" on page 625. The MAC address of the switch cannot be changed.the MAC address of the switch.

The root bridge parameter specifies the bridge identifier of the root bridge of the spanning tree domain. The identifier consists of the bridge or CIST priority value and MAC address of the root switch, separated by a slash (/). This parameter only appears when STP is activated on the switch.

The PORTCONFIG parameter displays the following MSTP port parameter settings:

- Edge-port status
- Point-to-point status
- External and internal port costs
- Port priority

The PORTSTATE parameter displays the following MSTP port status information:

- MSTP port state
- MSTP role
- Point-to-point status
- Spanning tree version
- Internal and external port costs

The MSTI parameter displays the following information for each spanning tree instance (excluding the CIST) on the switch:

❒ MSTI ID

❒ MSTI priority

❒ Regional root ID

❒ Path cost

❒ Associated VLANs

The CIST parameter displays the following CIST information:

❒ CIST priority value

❒ Root ID

❒ Root path cots

❒ Regional root ID

❒ Regional root path cost

❒ Associated VLANs

The MSTIVLANASSOC parameter displays the VLAN to MSTI associations.

Examples

This command displays basic MSTP operating information:

```
show mstp
```

This command displays the MSTP state of Port 4:

```
show mstp portstate=4
```

This command displays the configuration of Port 5 in MSTI 2:

```
show mstp portconfig=5 stpid=2
```

This command displays the CIST information:

```
show mstp cist
```

This command displays the VLAN associations:

```
show mstp mstivlanassoc
```

AlliedWare Plus Command

Syntax

```
show spanning-tree detail
show spanning-tree interface [port]
show spanning-tree mst config [port]
show spanning-tree mst detail
show spanning-tree mst instance
show spanning-tree mst association
```

Mode

User Exec mode and Privileged Exec mode

Description

Table 25 lists the AlliedWare Plus SHOW SPANNING-TREE parameters and their equivalent standard command parameters.

Table 25. SHOW SPANNING-TREE Command Options

AlliedWare Plus Command Parameter	Standard Command Parameter
DETAIL	This is equivalent to entering the SHOW MSTP command without any parameters.
INTERFACE	This is equivalent to the PORTSTATE parameter.
MST CONFIG	This is equivalent to the PORTCONFIG parameter.
MST DETAIL	This is equivalent to the MSTISTATE parameter.
MST INSTANCE	This is equivalent to the CIST parameter.
MST ASSOCIATION	This is equivalent to the MSTIVLANASSOC parameter.

The AlliedWare Plus interface does not have a command equivalent to the STPID parameter in the standard command.

Example

This command displays basic MSTP operating information:

```
awplus# show spanning-tree detail
```

This command displays the MSTP state of port 8:

```
awplus# show spanning-tree interface 8
```

This command displays the configuration of port 4:

```
awplus# show spanning-tree mst config 4
```

This command displays the CIST information:

```
show spanning-tree mst instance
```

This command displays the VLAN associations:

```
show spanning-tree mst association
```

Section VI

Virtual LANs

This section contains the following chapters:

Chapter 34

Port-based VLAN, Tagged VLAN, and Multiple VLAN Mode Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stack	Yes*
(*Stacks do not support the multiple VLAN modes.)	

This chapter contains the following commands:

ADD VLAN

AlliedWare Plus
Command
Available

Syntax 1

```
add vlan=name [vid=vid] ports=ports|all
frame=untagged|tagged
```

Syntax 2

```
add vlan=name [vid=vid] taggedports=ports|all
untaggedports=ports|all
```

Parameters

vlan Specifies the name of the VLAN to modify.

vid Specifies the VID of the VLAN you want to modify. This parameter is optional.

ports Specifies the ports to be added to the VLAN. You can add more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

frame Identifies the new ports as either tagged or untagged. This parameter must be used with the PORT parameter.

taggedports Specifies the ports to be added as tagged ports to the VLAN. To include all ports on the switch as tagged ports in the VLAN, use ALL.

untaggedports Specifies the ports to be added as untagged ports to the VLAN. Specifying ALL adds all ports on the switch as untagged ports to the VLAN.

Description

This command adds tagged and untagged ports to an existing port-based or tagged VLAN.

Note
To initially create a VLAN, see “CREATE VLAN” on page 647. To remove ports from a VLAN, see “DELETE VLAN” on page 651.

This command has two syntaxes. You can use either command to add ports to a VLAN. The difference between the two is that Syntax 1 can add only one type of port, tagged or untagged, at a time to a VLAN, while Syntax 2 can add both in the same command. This is illustrated in Examples below.

When you add untagged ports to a VLAN, the ports are automatically removed from their current untagged VLAN assignment. This is because a port can be an untagged member of only one VLAN at a time. For example, if you add port 4 as an untagged port to a VLAN, the port is automatically removed from whichever VLAN it is currently an untagged member.

Adding a tagged port to a VLAN does not change the port’s current tagged and untagged VLAN assignments. This is because a tagged port can belong to more than one VLAN at a time. For instance, if you add port 6 as an tagged port to a new VLAN, port 6 remains a tagged and untagged member of its other VLAN assignments.

If the switch is using 802.1x port-based network access control, a port set to the authenticator or supplicant role must be changed to the 802.1x none role before its untagged VLAN assignment can be changed. After the VLAN assignment is made, the port’s role can be changed back again to authenticator or supplicant, if necessary.

Examples

The following command uses Syntax 1 to add ports 4 and 7 as untagged members to a VLAN called Sales:

```
add vlan=sales ports=4,7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
add vlan=sales untaggedports=4,7
```

The following command uses Syntax 1 to add port 3 as a tagged member to a VLAN called Production:

```
add vlan=production ports=3 frame=tagged
```

The following command does the same thing using Syntax 2:

```
add vlan=production untaggedports=3
```

Adding both tagged and untagged ports to a VLAN using Syntax 1 takes two commands, one command for each port type. For example, if you had a VLAN called Service and you wanted to add port 5 as a tagged port and ports 7 and 8 as untagged ports, the commands would be:

```
add vlan=Service ports=5 frame=tagged
add vlan=Service ports=7-8 frame=untagged
```

Using Syntax 2, you can add both types of ports with just one command:

```
add vlan=Service untaggedports=7-8 taggedports=5
```

AlliedWare Plus Command

Syntax

To add untagged ports:

```
switchport access vlan vid
```

To add tagged ports:

```
switchport trunk allow vlan add vid
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example adds ports 5 and 7 as untagged ports to a VLAN with the VID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5,7
awplus(config-if)# switchport access vlan 12
```

This example adds ports 18 to 21 and 24 as tagged ports to a VLAN with the VID 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18-21,24
awplus(config-if)# switchport trunk allow vlan add 7
```

CREATE VLAN

AlliedWare Plus Command Available

Syntax 1

```
create vlan=name vid=vid [type=port] ports=ports|all
frame=untagged|tagged
```

Syntax 2

```
create vlan=name vid=vid [type=port] taggedports=ports|all
untaggedports=ports|all
```

Parameters

vlan

Specifies the name of the VLAN. You must assign a name to a VLAN.

The name can be from 1 to 20 characters in length and should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

The name cannot be the same as the name of an existing VLAN on the switch.

If the VLAN is unique in your network, then the name needs to be unique as well. If the VLAN spans multiple switches, then the name for the VLAN should be the same on each switch.

vid

Specifies the VLAN identifier. The range is 2 to 4094. The VLAN must be assigned a VID.

You cannot use the VID 1, which is reserved for the Default_VLAN.

The VID cannot be the same as the VID of an existing VLAN on the switch.

If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, assign the Sales VLAN on each switch the same VID value.

type — Specifies the type of VLAN to be created. The option PORT signifies a port-based or tagged VLAN. This parameter is optional.

ports — Specifies the ports of the VLAN. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48. To specify all the ports, use ALL. This parameter must be followed by the FRAME parameter.

frame — Specifies whether the ports are to be tagged or untagged. This parameter must be used with the PORT parameter.

taggedports — Specifies the tagged ports of the VLAN. To specify all ports, use ALL. Omit this parameter if the VLAN does not contain tagged ports.

untaggedports — Specifies the untagged ports of the VLAN. To specify all the ports, use ALL. Omit this parameter if the VLAN does not contain untagged ports.

Description

This command is used to create port-based and tagged VLANs.

This command has two syntaxes. You can use either syntax to create VLANs. The difference between the two syntaxes is how you specify the tagged and untagged ports. Syntax 1 is limited because it allows you to specify either tagged or untagged ports, but not both at the same time. On the other hand, you can use Syntax 2 to create a VLAN that has both types of ports. This is illustrated in the Examples section below.

When you create a new VLAN, untagged ports of the new VLAN are automatically removed from their current untagged VLAN assignment. This is because a port can be an untagged member of only one VLAN at a time. For example, creating a new VLAN with untagged Ports 1 to 4 automatically removes these ports from whichever VLAN they are currently untagged members.

The PVID of an untagged port is automatically changed to match the VID number of the VLAN where it is added. For instance, if you add port 4 as an untagged member of a VLAN with a VID of 15, the PVID for port 4 is automatically changed to 15.

Tagged ports of the new VLAN remain as tagged and untagged members of their current VLAN assignments. No change is made to a tagged port’s current VLAN assignments, other than its addition to the new VLAN. This is because a tagged port can belong to more than one VLAN at a time. For example, if you add port 6 as a tagged port to a new VLAN, port 6 remains a member of its other current untagged and tagged VLAN assignments.

If the switch is using 802.1x port-based network access control, a port set to the authenticator or supplicant role must be changed to the 802.1x none role before its untagged VLAN assignment can be changed. After the VLAN assignment is made, the port’s role can be changed back again to authenticator or supplicant, if necessary.

Examples

The following command uses Syntax 1 to create a port-based VLAN called Sales with a VID of 3. The VLAN consists of ports 4 to 8 and ports 12 to 16. All ports will be untagged ports in the VLAN:

```
create vlan=Sales vid=3 ports=4-8,12-16 frame=untagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan=Sales vid=3 untaggedports=4-8,12-16
```

In the following command, Syntax 1 is used to create a tagged VLAN called Production with a VID of 22. The VLAN consists of two tagged ports, ports 3 and 6:

```
create vlan=Production vid=22 ports=3,6 frame=tagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan=Sales vid=22 taggedports=3,6
```

You cannot use Syntax 1 to create a tagged VLAN that contains both untagged and tagged ports. For instance, suppose you wanted to create a VLAN called Service with a VID of 16 and untagged ports 1, 4, 5-7 and tagged ports 11 and 12. Creating this VLAN using Syntax 1 would actually require two commands. You would first need to create the VLAN, specifying either the untagged or tagged ports. As an example, the following command creates the VLAN and specifies the untagged ports:

```
create vlan=Service vid=16 ports=1,4,5-7 frame=untagged
```

Then, to add the other ports (in this case tagged ports), you would need to use the ADD VLAN command.

Syntax 2 allows you to create a VLAN of both tagged and untagged ports all in one command. Here is the command that would create our example:

```
create vlan=Service vid=16 untaggedports=1,4,5-7
taggedports=11-12
```

The advantage of Syntax 2 over Syntax 1 is that you can create VLANs that contain both types of ports with one command rather than two commands.

AlliedWare Plus Command

Syntax

```
vlan name vid vid
```

Mode

VLAN Configuration mode

Description

To create a new VLAN with the AlliedWare Plus commands, you perform two steps. In the first step you create the VLAN by assigning it a name and a VID with this command in the VLAN Configuration mode. Then you go to the Port Interface mode and assign the tagged and untagged ports. The commands for assigning the ports are described in the AlliedWare Plus command in “ADD VLAN” on page 644.

Example

This example creates the Engineering VLAN and assigns it the VID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# vlan Engineering vid 5
```

DELETE VLAN

AlliedWare Plus Command Available

Syntax 1

```
delete vlan=name [vid=vid] ports=ports frame=untagged|tagged
```

Syntax 2

```
delete vlan=name [vid=vid] taggedports=ports
untaggedports=ports
```

Parameters

vlan	Specifies the name of the VLAN to be modified.
vid	Specifies the VID of the VLAN to be modified. This parameter is optional.
ports	Specifies the ports to be removed from the VLAN. This parameter must be used with the FRAME parameter.
frame	Identifies the ports to be removed as tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the tagged ports to be removed from the VLAN.
untaggedports	Specifies the untagged ports to be removed from the VLAN.

Description

This command removes tagged and untagged ports from a port-based or tagged VLAN.

This command has two syntaxes. You can use either command to delete ports from a VLAN. The difference between the two is that Syntax 1 can remove only one type of port, tagged or untagged, at a time from a VLAN, while Syntax 2 allows you to remove both port types in the same command. This is illustrated in the Examples section below.

Note
To delete a VLAN, see "DESTROY VLAN" on page 654.

Note
You cannot change a VLAN’s name or VID.

When you remove an untagged port from a VLAN, the following happens:

❒ The port is returned to the Default_VLAN as an untagged port.

❒ If the port is also a tagged member of other VLANS, those VLAN assignments are not changed. The port remains a tagged member of the other VLANs. For example, if you remove Port 4 from a VLAN, the port is automatically returned as an untagged port to the Default VLAN. If Port 4 is functioning as a tagged member in one or more other VLANs, it remains as a tagged member of those VLANs.

❒ If you remove an untagged port from the Default_VLAN without assigning it to another VLAN, the port is excluded as an untagged member from all VLANs on the switch.

When you remove a tagged port from a VLAN, all of its other tagged and untagged VLAN assignments remain unchanged.

If the switch is using 802.1x port-based network access control, a port set to the authenticator or supplicant role must be changed to the 802.1x none role before its untagged VLAN assignment can be changed. After the VLAN assignment is made, the port’s role can be changed back again to authenticator or supplicant, if necessary.

Examples

The following command uses Syntax 1 to delete untagged ports 4 and 7 from a VLAN called Sales:

```
delete vlan=sales ports=4,7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
delete vlan=sales untaggedports=4,7
```

The following command uses Syntax 1 to delete tagged port 13 from a VLAN called Production:

```
delete vlan=production ports=13 frame=tagged
```

The following command does the same thing using Syntax 2:

```
delete vlan=production untaggedports=13
```

To delete both tagged and untagged ports from a VLAN using Syntax 1 takes two commands. For example, if you had a VLAN called Service and you wanted to delete tagged port 2 and untagged ports 6 to 8, the commands would be:

```
delete vlan=Service ports=2 frame=tagged
```

```
delete vlan=Service ports=6-8 frame=untagged
```

Using Syntax 2, you can do the whole thing with just one command:

```
delete vlan=Service untaggedports=6-8 taggedports=2
```

AlliedWare Plus Command

Syntax

To remove untagged ports:

```
no switchport access vlan
```

To remove tagged ports:

```
switchport trunk allow vlan remove vid
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example removes untagged port 5 from its VLAN and returns it to the Default VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5
awplus(config-if)# no switchport access vlan
```

This example removes tagged ports 18 and 19 from a VLAN with the VID 7:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 18,19
awplus(config-if)# switchport trunk allow vlan remove 7
```

DESTROY VLAN

AlliedWare Plus
Command
Available

Syntax

```
destroy vlan=name|vid|all
```

Parameters

vlan Specifies the name or VID of the VLAN to be deleted. To delete all VLANs, use the ALL option.

Description

This command deletes port-based, tagged, and MAC address-based VLANs from a switch. You can use the command to delete selected VLANs or all the VLANs on the switch. Note the following before using this command:

- You cannot delete the Default_VLAN.
- You cannot delete a VLAN if it has a routing interface. You must first delete the interface from the VLAN. To delete an interface, refer to “DELETE IP INTERFACE” on page 720.
- All untagged ports in a deleted VLAN are returned to the Default_VLAN as untagged ports.
- Static addresses assigned to the ports of a deleted VLAN become obsolete and should be deleted from the MAC address table. For instructions, refer to “DELETE SWITCH FDB|FILTER” on page 194.
- You cannot delete a VLAN if it is a monitored interface of a VRRP. To remove the VLAN from a monitored interface, refer to “DELETE VRRP MONITOREDINTERFACE” on page 776.

Examples

The following command deletes the Sales VLAN from the switch:

```
destroy vlan=Sales
```

The following command deletes the Sales VLAN using both the name and the VID:

```
destroy vlan=Sales vid=102
```

The following command deletes all the port-based and tagged VLANs on a switch:

```
destroy vlan=all
```

AlliedWare Plus Command

Syntax

`no vlan` *`name`* `vid` *`vid`*

Mode

VLAN Configuration mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes the Engineering VLAN with the VID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# vlan database
awplus(config-vlan)# no vlan Engineering vid 5
```

SET SWITCH INFILTERING

Syntax

```
set switch infiltering=yes|no|on|off|true|false
```

Parameters

infiltering — Specifies the operating status of ingress filtering. The options are:

- yes, on, true — Activates ingress filtering. The options are equivalent. This is the default.
- no, off, false — Deactivates ingress filtering. The options are equivalent.

Description

This command controls the status of ingress filtering. When ingress filtering is activated, which is the default, tagged frames are filtered when they are received on a port. When ingress filtering is deactivated, tagged frames are filtered before they are transmitted out a port. To view the current setting, use the “SHOW SWITCH MODULE” on page 96. For further information on ingress filtering, refer to the *AT-S63 Management Software Menus Interface User’s Guide*.

Example

The following command deactivates ingress filtering:

```
set switch infiltering=off
```

SET SWITCH VLANMODE

Syntax

```
set switch vlanmode=userconfig|dotqmultiple|multiple
[uplinkport=port]
```

Parameters

vlanmode — Controls the switch's VLAN mode. Options are:

- userconfig — This mode allows you to create your own port-based and tagged VLANs. This is the default setting.
- dotqmultiple — This option configures the switch for the 802.1Q-compliant multiple VLAN mode.
- multiple — This option configures the switch for the non-802.1Q compliant multiple VLAN mode.

uplinkport — Specifies the port on the switch to function as the uplink port when the switch is operating in one of the two multiple VLAN modes. You can specify only one port.

Description

You use this command to configure the switch for one of the multiple VLAN modes or so that you can create port-based and tagged VLANs.

If you select one of the multiple VLAN modes, you must also set an uplink port with the UPLINKPORT parameter. You can specify only one uplink port.

Examples

The following command configures the switch for the 802.1Q-compliant multiple VLAN mode and specifies port 4 as the uplink port:

```
set switch vlanmode=dotqmultiple uplinkport=4
```

The following command sets the switch so that you can create your own port-based and tagged VLANs:

```
set switch vlanmode=userconfig
```

SET VLAN

Syntax

```
set vlan=name [vid=vid] type=portbased
```

Parameter

vlan — Specifies the name of the dynamic GVRP VLAN you want to convert into a static VLAN. To view VLAN names, refer to “SHOW VLAN” on page 659.

vid — Specifies the VID of the dynamic VLAN. To view VIDs, refer to “SHOW VLAN” on page 659. This parameter is optional.

type — Specifies the type of static VLAN to which the dynamic VLAN is to be converted. There is only one option: PORTBASED.

Description

This command converts a dynamic GVRP VLAN into a static tagged VLAN. You can perform this command to permanently retain the VLANs the switch learned through GVRP.

Note
This command cannot convert a dynamic GVRP port in a static VLAN into a static port. For that you must manually modify the static VLAN, specifying the dynamic port as either a tagged or untagged member of the VLAN.

Example

This command changes the dynamic VLAN GVRP_VLAN_22 into a static VLAN:

```
set vlan=gvrp_vlan_22 type=portbased
```

SHOW VLAN

AlliedWare Plus
Command
Available

Syntax

show vlan[=*name*|*vid*]

Parameter

vlan	Specifies the name or VID of the VLAN.

Description

This command displays the VLANs on the switch. An example of the information displayed by this command for port-based and tagged VLANs is shown in Figure 76.

```
VLAN Name ............................ Sales
VLAN ID .............................. 4
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s)
  Configured ......................... 2,8-12
  Actual ............................. 2,8-12
Tagged Port(s) ....................... 24


VLAN Name ............................ Engineering
VLAN ID .............................. 5
VLAN Type ............................ Port Based
Protected Ports ...................... No
Untagged Port(s)
  Configured ......................... 5-7
  Actual ............................. 5-7
Tagged Port(s) ....................... 24
```

Figure 76. SHOW VLAN Command for Port-based and Tagged VLANs

The information displayed by the command is described here:

- VLAN name - The name of the VLAN.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be Port Based for port-based and tagged VLANs.
- Protected Ports - The status of protected ports. Since port-based and tagged VLANs are not protected ports VLANs, this will be No.
- Untagged port(s) - The untagged ports of the VLAN. The untagged ports are listed as follows.
  - Configured: The untagged ports assigned to the VLAN when the VLAN was created or modified.

- Actual: The current untagged ports of the VLAN. If you are not using 802.1x port-based network access control, both the Configured and Actual untagged ports of a VLAN will always be the same.

  If you are using 802.1x and you assigned a guest VLAN to an authenticator port or you associated an 802.1x supplicant to a VLAN on the authentication server, it is possible for ports to be in different VLANs than the virtual LANs where they were originally assigned as untagged ports. In these situations, the Configured and Actual port lists can differ, with the Actual list detailing the ports that are currently functioning as untagged ports of the VLAN.

  For example, if a particular port is listed as a Configured member of a VLAN, but not as an Actual member, that would mean either the port is currently a part of a Guest VLAN or the supplicant who logged on the port was associated with a VLAN assignment on the authentication server.

❒ Tagged port(s) - The tagged ports of the VLAN. A tagged port can belong to more than one VLAN at a time.

An example of the information displayed by this command for the 802.1Q-compliant multiple VLAN mode is shown in Figure 77.

```
VLAN Mode: Pre Configured (802.1Q Multiple VLANs)
VLAN Information:

VLAN Name ............................. Client_VLAN_1
VLAN ID ............................... 1
VLAN Type ............................. Port Based
Protected Ports ....................... No
Untagged Port(s) ......................  1
Tagged Port(s) ........................ 23


VLAN Name ............................. Client_VLAN_2
VLAN ID ............................... 2
VLAN Type ............................. Port Based
Protected Ports ....................... No
Untagged Port(s) ...................... 2
Tagged Port(s) ........................ 23


VLAN Name ............................. Client_VLAN_3
VLAN ID ............................... 3
VLAN Type ............................. Port Based
Protected Ports ....................... No
Untagged Port(s) ...................... 3
Tagged Port(s) ........................ 23
```

Figure 77. SHOW VLAN Command for the 802.1Q-compliant Multiple VLAN Mode

The information displayed by the command is described here:

- VLAN name - The name of the VLAN. The name is Client_VLAN followed by the port number.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be Port Based for the VLANs of a multiple VLAN mode.
- Protected Ports - The status of protected ports. Since the VLANs of a multiple VLAN mode are not protected ports VLANs, this will be No.
- Untagged port(s) - The untagged port of the VLAN.
- Tagged port(s) - The tagged port that is functioning as the uplink port for the VLANs.

For an example of the information displayed by this command for a protected ports VLAN, see Figure 78 on page 691. For an example of a MAC address-based VLAN, see Figure 79 on page 701.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays information on just the Sales VLAN:

```
show vlan=sales
```

The following command displays information for the VLAN with the VID of 22:

```
show vlan=22
```

AlliedWare Plus Command

Syntax

```
show vlan all
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays all of the VLANs on the switch. You can use this command to display port-based and tagged VLANs, as well as the VLANs in the multiple VLAN modes. This command cannot display protected-ports VLANs or MAC address-based VLANs.

This command displays the following columns of information for port-based and tagged VLANs:

- ❒ VLAN name - The names of the VLANs.
- ❒ VLAN ID - The ID numbers of the VLANs.
- ❒ Type - The VLAN type. This will be Port Based for port-based VLANs and tagged VLANs.
- ❒ State - The states of the VLANs. The states are Active for VLANs that have ports and Inactive for VLANs that do not have ports.
- ❒ Member Ports - The untagged and tagged ports of the VLANs.

Example

```
awplus# show vlan all
```

Chapter 35

GARP VLAN Registration Protocol Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

DISABLE GARP

AlliedWare Plus Command Available

Syntax

```
disable garp=gvrp [gip]
```

Parameters

garp Specifies the GARP application to be disabled. GVRP is the only GARP application supported by the AT-9400 Switch.

gip Disables GARP Information Propagation (GIP).

> **Note**
> The online help for this command contains an STP option. The option is not supported.

Description

This command disables GVRP on the switch. When GVRP is disabled, the switch cannot learn dynamic GVRP VLANs or dynamic GVRP ports.

You can also use this command to disable GIP.

> **Note**
> Do not disable GIP if the switch is running GVRP. GIP is required for proper GVRP operation.

Examples

The following command disables GVRP on the switch:

```
disable garp=gvrp
```

The following command disables GIP only:

```
disable garp=gvrp gip
```

AlliedWare Plus Command

Syntax

To disable GVRP:

```
no gvrp enable
```

To disable GIP:

```
gvrp applicant state normal
```

or

```
no gvrp dynamic-vlan-creation
```

Mode

Configure mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

This example disables GVRP:

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp enable
```

This example disables GIP:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp applicant state normal
```

This example disables GIP:

```
awplus> enable
awplus# configure terminal
awplus(config)# no gvrp dynamic-vlan-creation
```

ENABLE GARP

AlliedWare Plus
Command
Available

Syntax

```
enable garp=gvrp [gip]
```

Parameters

garp — Specifies the GARP application to be activated. GVRP is the only GARP application supported by the AT-9400 Switch.

gip — Enables GARP Information Propagation (GIP).

> **Note**
> The online help for this command contains an STP option. This option is not supported.

Description

This command enables GVRP on the switch. After activated, the switch will learn dynamic GVRP VLANs and dynamic GVRP ports.

You can also use this command to enable GIP. GIP must be enabled for GVRP to operate properly.

Examples

The following command enables GVRP on the switch:

```
enable garp=gvrp
```

The following command enables GIP only:

```
enable garp=gvrp gip
```

AlliedWare Plus Command

Syntax

To enable GVRP:

```
gvrp enable
```

To enable GIP:

```
gvrp applicant state active
```

or

```
gvrp dynamic-vlan-creation enable
```

Mode

Configure mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

This example activates GVRP:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp enable
```

This example activates GIP:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp applicant state active
```

This example also activates GIP:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp dynamic-vlan-creation enable
```

PURGE GARP

Syntax

```
purge garp=gvrp
```

Parameter

garp	Specifies the GARP application to be reset. GVRP is the only GARP application supported by the AT-9400 Switch.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command disables GVRP and returns all GVRP parameters to their default settings. All GVRP-related statistics counters are returned to zero.

Example

The following command disables GVRP and returns all GVRP parameters to their default values:

```
purge garp=gvrp
```

SET GARP PORT

AlliedWare Plus Command Available

Syntax

```
set garp=gvrp port=port mode=normal|none
```

Parameters

garp — Specifies the GARP application to be configured. GVRP is the only GARP application supported by the AT-9400 Switch.

port — Specifies the port to be configured. You can specify more than one port at a time.

mode — Specifies the GVRP mode of the port. Modes are:

- normal — The port participates in GVRP. The port processes GVRP information and transmits PDUs. This is the default.
- none — The port does not participate in GVRP. The port does not process GVRP information or transmit PDUs.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command sets a port's GVRP status. Set a port's mode to Normal if it is to learn remote VLANs and transmit PDUs. Set its mode to None If it is not to participate in GVRP.

Examples

The following command prevents ports 1 to 4 from participating in GVRP:

```
set garp=gvrp port=1-4 mode=none
```

The following command activates GVRP on port 3:

```
set garp=gvrp port=3 mode=normal
```

AlliedWare Plus Command

Syntax

```
gvrp registration normal|none
```

Mode

Port Interface mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example configures ports 5 and 6 to participate in GVRP:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5,6
awplus(config-if)# gvrp registration normal
```

This example configures port 20 to not participate in GVRP:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 20
awplus(config-if)# gvrp registration none
```

SET GARP TIMER

AlliedWare Plus Command Available

Syntax

```
set garp=gvrp timer [default] [jointime=value]
[leavetime=value] [leavealltime=value]
```

Parameters

garp — Specifies the GARP application to be configured. GVRP is the only GARP application supported by the AT-9400 Switch.

default — Returns the GARP timers to their default settings.

jointime — Specifies the Join Timer in centiseconds, which are one hundredths of a second. The default is 20 centi seconds.

If you change this timer, it must be in relation to the GVRP Leave Timer according to the following equation:

Join Timer <= (2 x (GVRP Leave Timer))

leavetimer — Specifies the Leave Timer in centiseconds, which are one hundredths of a second. The default is 60 centi seconds.

leavealltime — Specifies the Leave All Timer in centiseconds. The default is 1000 centiseconds.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command sets the GARP timers.

Note
The settings for these timers must be the same on all GVRP-active network devices.

Examples

This command sets the Join Timer to 0.1 second, Leave Timer to 0.35 seconds, and the Leave All Timer to 11 seconds:

```
set garp=gvrp timer jointime=10 leavetime=35
leavealltime=1100
```

The following command sets the timers to their default values:

```
set garp=gvrp timer default
```

AlliedWare Plus Command

Syntax

To set the Join Timer:

```
gvrp timer join value
```

To set the Leave Timer:

```
gvrp timer leave value
```

To set the Leave All Timer:

```
gvrp timer leaveall value
```

Mode

Configure mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

This command sets the Join Timer to 0.2 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer join 20
```

This command sets the Leave Timer to 0.8 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer leave 80
```

This command sets the Leave All timer to 10 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# gvrp timer leaveall 1000
```

SHOW GARP

AlliedWare Plus Command Available

Syntax

```
show garp=gvrp
```

Parameter

garp	Specifies the GARP application to display. GVRP is the only GARP application supported by the AT-9400 Switch.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays the current values for the following GARP application parameters:

- GARP application protocol
- GVRP status
- GVRP GIP status
- GVRP Join Time
- GVRP Leave Time
- GVRP Leaveall Time
- Port information
- Mode

Example

The following command displays GVRP information:

```
show garp=gvrp
```

AlliedWare Plus Command

Syntax

```
show gvrp timer
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show gvrp timer
```

SHOW GARP COUNTER

AlliedWare Plus Command Available

Syntax

```
show garp=gvrp counter
```

Parameter

garp	Specifies the GARP application to be displayed. GVRP is the only GARP application supported by the AT-9400 Switch.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays the current values for the following GARP packet and message counters:

- ❐ GARP application
- ❐ Receive: Total GARP Packets
- ❐ Transmit: Total GARP Packets
- ❐ Receive: Invalid GARP Packets
- ❐ Receive Discarded: GARP Disabled
- ❐ Receive DIscarded: Port Not Listening
- ❐ Transmit Discarded: Port Not Sending
- ❐ Receive Discarded: Invalid Port
- ❐ Receive Discarded: Invalid Protocol
- ❐ Receive Discarded: Invalid Format
- ❐ Receive Discarded: Database Full
- ❐ Receive GARP Messages: LeaveAll
- ❐ Transmit GARP Messages: LeaveAll
- ❐ Receive GARP Messages: JoinEmpty
- ❐ Transmit GARP Messages: JoinEmpty
- ❐ Receive GARP Messages: JoinIn
- ❐ Transmit GARP Messages: JoinIn
- ❐ Receive GARP Messages: LeaveEmpty
- ❐ Transmit GARP Messages: LeaveEmpty

❒ Receive GARP Messages: LeaveIn

❒ Transmit GARP Messages: LeaveIn

❒ Receive GARP Messages: Empty

❒ Transmit GARP Messages: Empty

❒ Receive GARP Messages: Bad Message

❒ Receive GARP Messages: Bad Attribute

Example

The following command displays information for all GARP application counters:

```
show garp=gvrp counter
```

AlliedWare Plus Command

Syntax

```
show gvrp statistics
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show gvrp statistics
```

SHOW GARP DATABASE

AlliedWare Plus
Command
Available

Syntax

```
show garp=gvrp db|database
```

Parameters

garp

Specifies the GARP application to be displayed. GVRP is the only GARP application supported by the AT-9400 Switch.

Note
The online help for this command contains an STP option. This option is not supported.

Description

This command displays the following parameters for the internal database for the GARP application. Each attribute is represented by a GID index within the GARP application.

- GARP Application
- GID Index
- Attribute
- Used

Example

The following command displays the database for all GARP applications:

```
show garp=gvrp database
```

AlliedWare Plus Command

Syntax

```
show gvrp configuration
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show gvrp configuration
```

SHOW GARP GIP

AlliedWare Plus Command Available

Syntax

```
show garp=gvrp gip
```

Parameter

garp	Specifies the GARP application to be displayed. GVRP is the only GARP application supported by the AT-9400 Switch.

Note
The online help for this command contains an STP option. That option is not supported.

Description

This command displays the following parameters for the GIP-connected ring for the GARP application:

- ❒ GARP Application
- ❒ GIP contact
- ❒ STP ID

Example

The following command displays the GIP-connected ring for all GARP applications:

```
show garp=gvrp gip
```

AlliedWare Plus Command

Syntax

```
show gvrp applicant
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show gvrp applicant
```

SHOW GARP MACHINE

AlliedWare Plus
Command
Available

Syntax

```
show garp=gvrp machine
```

Parameter

garp Specifies the GARP application to be displayed. GVRP is the only GARP application supported by the AT-9400 Switch.

> **Note**
> The online help for this command contains an STP option. This option is not supported.

Description

This command displays the following parameters for the GID state machines for the GARP application. The output is shown on a per-GID index basis; each attribute is represented by a GID index within the GARP application.

- VLAN
- Port
- App
- Reg

Example

The following command displays GID state machines for all GARP applications:

```
show garp=gvrp machine
```

AlliedWare Plus Command

Syntax

```
show gvrp machine
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show gvrp machine
```

Chapter 36

Protected Ports VLAN Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

ADD VLAN GROUP

Syntax 1

```
add vlan=name|vid ports=ports frame=tagged|untagged
group=uplink|1..256
```

Syntax 2

```
add vlan=name|vid [taggedports=ports] [untaggedports=ports]
group=uplink|1..256
```

Parameters

vlan Specifies the name or VID of the protected ports VLAN where ports are to be added. You can identify the VLAN by either its name or VID.

ports Specifies the uplink port(s) or the ports of a group. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.. This parameter must be used with the FRAME parameter.

frame Identifies the new ports as either tagged or untagged. This parameter must be used with the PORTS parameter.

taggedports Specifies the tagged ports to be added to the VLAN.

untaggedports Specifies the untagged ports to be added to the VLAN.

group Specifies that the port(s) being added is an uplink port or belongs to a new group. If the port(s) being added is an uplink port, specify the UPLINK option. Otherwise, specify the group number for the port. The group range is 1 to 256. The number must be unique for each group on the switch.

Description

These commands perform two functions. One is to specify the uplink port of a protected ports VLAN. The other function is to add ports to groups within a VLAN.

Note the following before using this command:

❒ You must first create the protected ports VLAN by giving it a name and a VID before you can add ports. Creating a VLAN is accomplished with “CREATE VLAN PORTPROTECTED” on page 686.

- ❐ Both command syntaxes perform the same function. The difference is that with syntax 1 you can add ports of only one type, tagged or untagged, at a time. With syntax 2, you can add both at the same time.
- ❐ If you are adding an untagged port to a group, the port cannot be an untagged member of another protected port VLAN. It must be an untagged member of the Default_VLAN or a port-based or tagged VLAN. To remove a port from a protected port VLAN, use "DELETE VLAN" on page 687.
- ❐ You cannot add a new uplink port to a VLAN if the VLAN has already been assigned an uplink port. Instead, you must delete the existing uplink port(s) using the "DELETE VLAN" on page 687 and then re-add the uplink port(s) using this command.
- ❐ You cannot add ports to an existing group. To modify an existing group, you must delete the group by removing all ports from it, using "DELETE VLAN" on page 687, and then add the ports back to the group using this command.

Examples

The following command uses Syntax 1 to specify that port 11 is to be an untagged uplink port for the protected ports VLAN called InternetGroups:

```
add vlan=InternetGroups ports=11 frame=untagged group=uplink
```

The following command accomplishes the same thing using Syntax 2:

```
add vlan=InternetGroups untaggedports=11 group=uplink
```

The following command uses Syntax 1 to create group 4 in the InternetGroups VLAN. The group will consist of two untagged ports, 5 and 6:

```
add vlan=InternetGroups port=5,6 frame=untagged group=4
```

The following command does the same thing using Syntax 2:

```
add vlan=InternetGroups untaggedports=5,6 group=4
```

CREATE VLAN PORTPROTECTED

Syntax

```
create vlan=name vid=vid portprotected
```

Parameters

vlan	Specifies the name of the new protected ports VLAN. The name can be from one to fifteen alphanumeric characters in length. The name should reflect the function of the nodes that will be a part of the protected ports VLAN (for example, InternetGroups). The name cannot contain spaces or special characters, such as an asterisk (*) or exclamation point (!).
vid	Specifies a VID for the new protected ports VLAN. The range is 2 to 4094. This number must be unique from the VIDs of all other tagged, untagged, and port protected VLANs on the switch.

Description

This command is the first step to creating a protected ports VLAN. This command assigns a name and VID to the VLAN. The second step is to specify an uplink port and the port groups using “ADD VLAN GROUP” on page 684.

Examples

The following command creates a protected ports VLAN called InternetGroups and assigns it a VID of 12:

```
create vlan=InternetGroups vid=12 portprotected
```

DELETE VLAN

Syntax 1

```
delete vlan=name|vid ports=ports frame=tagged|untagged
```

Syntax 2

```
delete vlan=name|vid [taggedports=ports]
[untaggedports=ports]
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified. You can specify the VLAN by its name or VID.
port	Specifies the port to be removed from the VLAN. You can specify more than one port at a time. This parameter must be used with the FRAME parameter.
frame	Identifies the ports to be removed as tagged or untagged. This parameter must be used with the PORT parameter.
taggedports	Specifies the tagged ports to be removed from the VLAN.
untaggedports	Specifies the untagged ports to be removed from the VLAN.

Description

This command removes ports from protected ports VLANs. You can use this command to remove uplink ports and ports from groups.

Note the following before using this command:

- Both command syntaxes perform the same function. The difference is that with Syntax 1 you can delete ports of only one type, tagged or untagged, at a time. With Syntax 2, you can delete both types at the same time.
- Deleting all ports from a group deletes the group from the VLAN.
- Deleted untagged ports are returned to the Default_VLAN as untagged.
- You can delete ports from only one group at a time.

Examples

The following command uses Syntax 1 to delete untagged port 12 from the InternetGroups VLAN:

```
delete vlan=InternetGroups port=12 frame=untagged
```

The following command accomplishes the same thing using Syntax 2:

```
delete vlan=InternetGroups untaggedports=12
```

DESTROY VLAN

Syntax

```
destroy vlan=name|vid|all
```

Parameters

vlan	Specifies the name or VID of the VLAN to be destroyed. To delete all tagged, port-based, and protected ports VLANs on the switch, use the ALL option.

Description

This command deletes VLANs from the switch. You can use this command to delete tagged, port-based, and protected port VLANs. All untagged ports in a deleted VLAN are automatically returned to the Default_VLAN. You cannot delete the Default_VLAN.

Example

The following command deletes the VLAN called InternetGroups:

```
destroy vlan=InternetGroups
```

The following command deletes all VLANs:

```
destroy vlan=all
```

SET VLAN

Syntax

```
set vlan=name|vid port=ports frame=tagged|untagged
```

Parameters

vlan — Specifies the name or VID of the VLAN to be modified.

ports — Specifies the port whose VLAN type is to be changed. You can specify more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

frame — Identifies the new VLAN type for the port. The type can be tagged or untagged.

Description

This command changes a port’s VLAN type. You can use this command to change a tagged port to untagged and vice versa.

Before using this command, note the following:

- Changing a port in a port-based, tagged, or protected ports VLAN from untagged to tagged adds the port to the Default_VLAN as untagged.
- Changing a port in the Default_VLAN from untagged to tagged results in the port being an untagged member of no VLAN.
- Changing a port from tagged to untagged removes the port from its current untagged port assignment.

Examples

The following command changes port 4 in the Sales VLAN from tagged to untagged:

```
set vlan=Sales port=4 frame=untagged
```

SHOW VLAN

Syntax

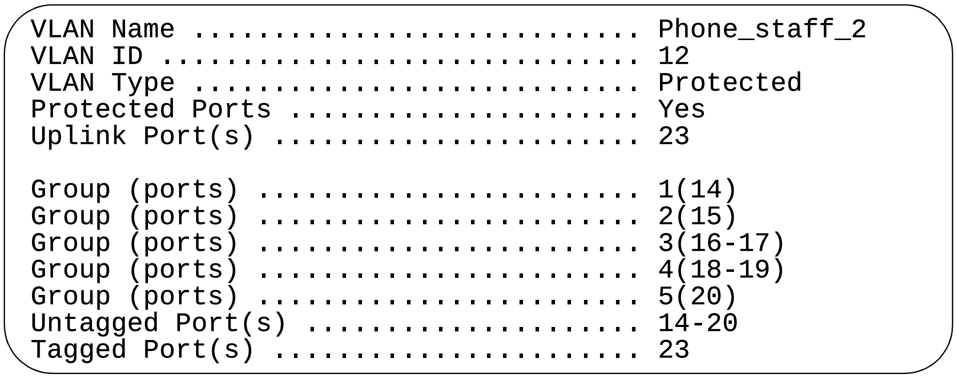
```
show vlan[=name|vid]
```

Parameter

vlan Specifies the name or VID of the VLAN you want to view. Omitting this displays all VLANs.

Description

This command displays information about the VLANs on the switch. An example of the information displayed by this command for a protected ports VLAN is shown in Figure 78.



```
VLAN Name ............................ Phone_staff_2
VLAN ID .............................. 12
VLAN Type ............................ Protected
Protected Ports ...................... Yes
Uplink Port(s) ....................... 23

Group (ports) ........................ 1(14)
Group (ports) ........................ 2(15)
Group (ports) ........................ 3(16-17)
Group (ports) ........................ 4(18-19)
Group (ports) ........................ 5(20)
Untagged Port(s) ..................... 14-20
Tagged Port(s) ....................... 23
```

Figure 78. SHOW VLAN Command for a Protected Ports VLAN

The information displayed by this command is described here:

- VLAN name - The name of the VLAN.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be Protected for a protected ports VLAN.
- Protected Ports - The status of protected ports. This will be Yes for a protected ports VLANs.
- Uplink Port(s) - The port that is functioning as the unlink port for the groups of the VLAN. There can be more than one uplink port.
- Group (ports) - The group number followed by the ports of the group.
- Untagged port(s) - The untagged ports of the VLAN.
- Tagged port(s) - The tagged ports of the VLAN.

For an example of the information displayed by this command for a port-based or tagged VLAN, see Figure 76 on page 659. For an example of a MAC address-based VLAN, see Figure 79 on page 701.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays the Sales VLAN:

```
show vlan=Sales
```

Chapter 37

MAC Address-based VLAN Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

ADD VLAN MACADDRESS

Syntax

```
add vlan=name|vid macaddress|destaddress=mac-address
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
macaddress ***or*** destaddress	Specifies the MAC address to add to the VLAN. These parameters are equivalent. A MAC address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command adds a MAC address to a MAC address-based VLAN. You can add only one address at a time with this command. The command does not accept ranges or wildcards.

The VLAN must already exist. To create a MAC address-based VLAN, see “CREATE VLAN TYPE=MACADDRESS” on page 696. After you add a MAC address to a VLAN, you can assign it one or more egress ports using “ADD VLAN PORT MACADDRESS” on page 695.

Examples

The following command adds the MAC address 00:30:84:32:8A:5D to the Sales VLAN:

```
add vlan=sales macaddress=00:30:84:32:8a:5d
```

The following command adds the MAC address 00:30:84:32:76:1A to the VLAN with the VID 12:

```
add vlan=12 macaddress=00308432761a
```

ADD VLAN PORT MACADDRESS

Syntax

```
add vlan=name|vid port=ports macaddress|destaddress=mac-
address
```

Parameters

vlan — Specifies the name or VID of the VLAN to be modified.

port — Specifies the egress port(s) to assign to the MAC address. You can specify more than one egress port.

macaddress ***or*** destaddress — Specifies the MAC address to be assigned the egress port(s). The MAC address can be entered in either of the following formats:

xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command assigns egress ports to MAC addresses in MAC address-based VLANs. A MAC address must already be in a VLAN before you can assign it egress ports. To assign a MAC address to a VLAN, refer to “ADD VLAN MACADDRESS” on page 694.

Examples

The following command assigns ports 1 and 4 as egress ports for the MAC address 00:30:84:32:8A:5D in the Sales VLAN:

```
add vlan=sales port=1,4 macaddress=00:30:84:32:8a:5d
```

The following command assigns port 11 to 14 as egress ports for the MAC address 00:30:84:75:11:B2 from the VLAN with the VID 24:

```
add vlan=24 port=11-14 macaddress=00:30:84:75:11:b2
```

CREATE VLAN TYPE=MACADDRESS

Syntax

```
create vlan=name vid=vid type=macaddress
```

Parameters

vlan

Specifies the name of the VLAN. You must assign a name to a VLAN.

The name can be from 1 to 20 characters in length and should reflect the function of the nodes that will be a part of the VLAN (for example, Sales or Accounting). The name cannot contain spaces or special characters, such as asterisks (*) or exclamation points (!).

The name cannot be the same as the name of an existing VLAN on the switch.

If the VLAN is unique in your network, then the name needs to be unique as well. If the VLAN spans multiple switches, then the name for the VLAN should be the same on each switch.

vid

Specifies the VLAN identifier. The range is 2 to 4094. The VLAN must be assigned a VID.

You cannot use the VID 1, which is reserved for the Default_VLAN.

The VID cannot be the same as the VID of an existing VLAN on the switch.

If this VLAN is unique in your network, then its VID should also be unique. If this VLAN is part of a larger VLAN that spans multiple switches, then the VID value for the VLAN should be the same on each switch. For example, if you are creating a VLAN called Sales that spans three switches, assign the Sales VLAN on each switch the same VID value.

type

Specifies the type of VLAN. To create a MAC address-based VLAN, the type must be MACADDRESS.

Description

This command is the first in the series to creating a MAC address-based VLAN. This command assigns the VLAN a name and a VID and sets the VLAN type. After you have initially created the VLAN with this command, you must assign the MAC addresses. These are the source addresses of the nodes that are to belong to the VLAN. The command for adding MAC addresses to a VLAN is “ADD VLAN MACADDRESS” on page 694.

The final step to creating a new MAC address-based VLAN is assigning the egress ports to the MAC addresses. The command for this is “ADD VLAN PORT MACADDRESS” on page 695.

Examples

The following command creates a MAC address-based VLAN called Sales and assigns it a VID of 3:

```
create vlan=Sales vid=3 type=macaddress
```

DELETE VLAN MACADDRESS

Syntax

```
delete vlan=*name*|*vid* macaddress|destaddress=*mac-address*
```

Parameters

vlan	Specifies the name or VID of the VLAN to be modified.
macaddress ***or*** destaddress	Specifies the MAC address to be removed from the VLAN. These parameters are equivalent. You can remove only one MAC address at a time. A MAC address can be entered in either of the following formats: xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command removes MAC addresses from a MAC address-based VLAN. You can remove only one MAC address at a time with this command.

You cannot remove a MAC address if it has been assigned egress ports. You must first remove the ports from the MAC address before you can delete it. To remove egress ports from a MAC address, refer to “DELETE VLAN PORT MACADDRESS” on page 699.

Examples

The following command removes the MAC address 00:30:84:32:8A:5D from the Sales VLAN:

```
delete vlan=Sales macaddress=00:30:84:32:8A:5D
```

The following command removes the MAC address 00:30:84:75:11:B2 from the VLAN with the VID 24:

```
delete vlan=24 macaddress=0030847511b2
```

DELETE VLAN PORT MACADDRESS

Syntax

```
delete vlan=name|vid port=ports macaddress=mac-address
```

Parameters

vlan Specifies the name or VID of the VLAN to be modified.

port Specifies the egress port to be removed for the MAC address. You can remove more than one egress port at a time.

macaddress Specifies a MAC address to which the port is assigned. A MAC address can be entered in either of the following formats:

xx:xx:xx:xx:xx:xx or xxxxxxxxxxxx

Description

This command removes egress ports from a MAC address of a MAC address-based VLAN. You might remove an egress port from a MAC address-based VLAN if you no longer want it to be a part of the VLAN.

Examples

The following command removes port 4 from the MAC address 00:30:84:32:8A:5D in the Sales VLAN:

```
delete vlan=Sales port=4 macaddress=00:30:84:32:8A:5D
```

The following command removes ports 11 to 14 from the MAC address 00:30:84:75:11:B2 in the VLAN with the VID 24:

```
delete vlan=24 port=11-14 macaddress=0030847511b2
```

DESTROY VLAN

Syntax

```
destroy vlan vlan=name|all [vid=vid]
```

Parameters

vlan Specifies the name of the VLAN to be deleted. To delete all VLANs, use the ALL option.

vid Specifies the VID of the VLAN to be deleted. This parameter is optional.

Description

The command deletes port-based, tagged, and MAC address-based VLANs. You can use the command to deleted selected VLANS or to delete all VLANs, with the exception of the Default_VLAN.

Examples

The following command deletes the Sales VLAN from the switch:

```
destroy vlan vlan=Sales
```

The following command deletes the Sales VLAN using both the name and the VID:

```
destroy vlan vlan=Sales vid=102
```

The following command deletes all port-based and tagged VLANs on a switch:

```
destroy vlan=all
```

SHOW VLAN

Syntax

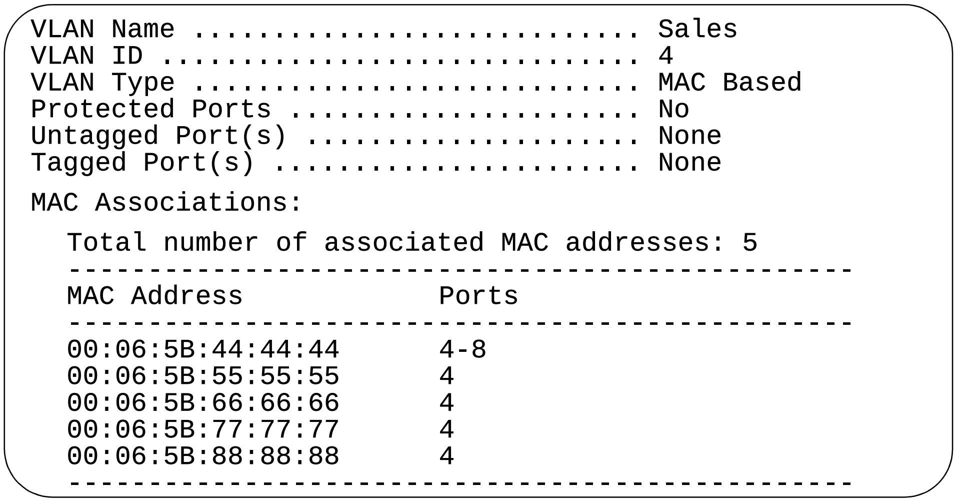
```
show vlan[=name|vid]
```

Parameter

vlan Specifies the name or VID of the VLAN.

Description

This command displays the VLANs on the switch. An example of the information displayed by this command for a MAC address-based VLAN is shown in Figure 79.



```
VLAN Name ............................ Sales
VLAN ID .............................. 4
VLAN Type ............................ MAC Based
Protected Ports ...................... No
Untagged Port(s) ..................... None
Tagged Port(s) ....................... None

MAC Associations:

  Total number of associated MAC addresses: 5
  ------------------------------------------------
  MAC Address            Ports
  ------------------------------------------------
  00:06:5B:44:44:44      4-8
  00:06:5B:55:55:55      4
  00:06:5B:66:66:66      4
  00:06:5B:77:77:77      4
  00:06:5B:88:88:88      4
  ------------------------------------------------
```

Figure 79. SHOW VLAN Command for a MAC Address-based VLAN

The information displayed by the command is described here:

- VLAN name - The name of the VLAN.
- VLAN ID - The ID number assigned to the VLAN.
- VLAN Type - The type of VLAN. This will be MAC Based for a MAC address-based VLAN.
- Protected Ports - The status of protected ports. This will be No for a MAC address-based VLAN.
- Untagged port(s) - The untagged ports of the VLAN. This will be None for a MAC address-based VLAN.
- Tagged port(s) - The tagged ports of the VLAN. This will be None for a MAC address-based VLAN.

- ❐ MAC Address / Ports - The MAC addresses of the VLAN and the egress ports.

For an example of the information displayed by this command for a port-based or tagged VLAN, see Figure 76 on page 659. For an example of a protected ports VLAN, see Figure 78 on page 691.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays information on only the Sales VLAN:

```
show vlan=sales
```

The following command displays information the VLAN with the VID of 22:

```
show vlan=22
```

Section VII

Internet Protocol Routing

This section contains the following chapters:

Chapter 38

Internet Protocol Version 4 Packet Routing Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	*
AT-9424T/GB	*
AT-9424T/SP	*
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes**

(*The Layer 2+ switches support one routing interface as an IP address.)

(**Stacks support static routes but not the Routing Information Protocol.)

This chapter has the following commands:

ADD IP ARP

AlliedWare Plus Command Available

Syntax

```
add ip arp=ipaddress interface=interface port=port
ethernet=macaddress
```

Parameters

arp — Specifies the IP address of the host. The IP address must be a member of a local subnet or network that has a routing interface on the switch.

interface — Specifies the name of the interface from where the host is reached. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

port — Specifies the physical port on the switch where the host is reached.

ethernet — Specifies the MAC address of the host. The MAC address can be entered in either of the following formats:

xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

Description

This command adds static ARP entries to the ARP cache. This is typically used to add entries for local hosts that do not support ARP or to speed up the address resolution function for a host. The ARP entry must not already exist in the cache. The switch can support up to 1024 static ARP entries.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP Switches.

Examples

This command adds a static ARP entry for a host with an IP address of 149.42.67.8 and a MAC address of 00:06:5B:BB:72:88. The host is a member of the subnet of the VLAN8-0 interface and is located on port 15:

```
add ip arp=149.42.67.8 interface=vlan8-0 port=15
ethernet=00:06:5b:bb:72:88
```

This command adds a static ARP entry for a host with an IP address of 149.124.85.14 and a MAC address of 00:06:7A:22:11:A4. The host is located on port 6 in the VLAN14-1 interface:

```
add ip arp=149.124.85.14 interface=vlan14-1 port=6
ethernet=00:06:7a:22:11:a4
```

AlliedWare Plus Command

Syntax

arp *ipaddress macaddress port*

Mode

Configure mode

Description

This command does not let you specify an interface number and assumes the ID 0. Thus, you can only use this command to add ARP entries to interfaces with the ID 0, like VLAN1-0 and VLAN2-0. To add ARP entries to interfaces that have other ID numbers, use the ADD IP ARP command in the standard command line interface.

Examples

This example creates an ARP entry for the IP address 149.22.23.12 and the MAC address 7A:54:2B:11:65:72 on port 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# arp 149.22.23.12 7a:54:2b:11:65:72 15
```

This example creates an ARP entry for the IP address 173.114.12.7 and the MAC address 7A:2C:8A:18:A1:12 on port 17:

```
awplus> enable
awplus# configure terminal
awplus(config)# arp 173.114.12.7 7a:2c:8a:18:a1:12 17
```

ADD IP INTERFACE

AlliedWare Plus Command Available

Syntax

```
add ip interface=interface ipaddress=ipaddress|dhcp|bootp
[mask|netmask=subnetmask] [ripmetric=value]
```

Parameters

interface — Specifies a name for the new routing interface. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). The range of the interface number is 0 to 15.

ipaddress — Specifies an IP address for the interface. The address must be a unique member of the subnet or network where the interface is to be assigned.

You can assign an address manually or activate the DHCP or BOOTP client and have a DHCP or BOOTP server on the network assign the address automatically. When there is more than one interface in a VLAN, only one of the interfaces can obtain its IP address from a DHCP or BOOTP server. The IP addresses of the other interfaces in the same VLAN must be assigned manually.

mask **or** netmask — Specifies the subnet mask of the IP address of the routing interface. Do not specify a mask if the IP address will be assigned by a DHCP or BOOTP server. The default value is based on the address’ network type. The default values are:

Class A address - 255.0.0.0

Class B address - 255.255.0.0

Class C address - 255.255.255.0

Note
In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the “1” bits are consecutive (e.g.,128, 192, 224, etc.).

ripmetric — Specifies the cost of crossing the interface for RIP. The range is 1 to 16. The default is 1.

Description

This command is used to create new interfaces for routing IPv4 packets to a local network or subnet. Note the following before using this command:

❒ The VLAN of a routing interface must already exist on the switch.

❒ You cannot assign more than one interface to the same local network or subnet on a switch.

❒ When there are multiple interfaces within a VLAN, each must be assigned a unique interface number.

❒ Only one interface in a VLAN can obtain its IP configuration from a DHCP or BOOTP server.

❒ If an interface is configured to use the DHCP or BOOTP client to obtain its IP address and subnet mask, it does not participate in IP routing until its IP address and subnet mask are received from the DHCP or BOOTP server.

❒ The AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches support only one routing interface.

Examples

This command creates an interface with an IP address 149.123.44.56 and a mask of 255.255.255.0. The interface is assigned to the VLAN with the VID of 6 and given the interface number 0. Since no RIP metric is specified, the default value of 1 is applied to the interface:

```
add ip interface=vlan6-0 ipaddress=149.123.44.56
netmask=255.255.255.0
```

This command creates an interface with an IP address 149.211.126.14 and a mask of 255.255.240.0. The interface is assigned to the VLAN with the VID of 24 and given the interface number 2. The RIP hop count for the interface is set to 2:

```
add ip interface=vlan24-2 ipaddress=149.211.126.14
netmask=255.255.240.0 ripmetric=2
```

This command creates an interface with an IP address and subnet mask set by a DHCP server. The interface is assigned to the VLAN with the VID of 18 and given the interface number 1. The hop count for RIP is increased to 4:

```
add ip interface=vlan18-1 ipaddress=dhcp ripmetric=4
```

AlliedWare Plus Command

Syntax

```
interface default_vlan
ip address ipaddress/mask|dhcp|bootp
rip-metric value
```

Mode

VLAN Interface mode

Description

This command has the following rules and restrictions:

- You can use this command to add a routing interface only to the Default_VLAN. To add routing interfaces to other VLANs on the switch, use the standard command.
- You cannot assign a name to a new routing interface.
- The command does not allow you to specify a routing interface number. The interface is automatically assigned the designation “VLAN1-0.” To create more than one routing interface in the Default_VLAN, use the standard command.

Examples

This example creates a routing interface with the IP address 149.22.23.12 and the mask 255.255.255.0 in the Default_VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface Default_VLAN
awplus(config-if)# ip address 149.22.23.12/24
```

This example creates a routing interface in the Default_VLAN, with the IP address 132.111.43.12, the mask 255.255.255.0, and the RIP metric 3:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface Default_VLAN
awplus(config-if)# ip address 132.111.43.12/24
awplus(config-if)# rip-metric 3
```

ADD IP RIP

AlliedWare Plus Command Available

Syntax

```
add ip rip interface=interface [send=rip1|rip2]
[receive=rip1|rip2|both] [authentication=pass|none]
[password=password]
[poisonreverse=yes|no|on|off|true|false]
[autosummary=yes|no|on|off|true|false]
```

Parameters

interface — Specifies the name of the routing interface where RIP is to be added. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

send — Specifies the version of RIP packets to be sent by the routing protocol. Options are:

- rip1 — Sends RIP version 1 packets. This is the default value.
- rip2 — Sends RIP version 2 packets.

receive — Specifies the version of RIP packets to be accepted by the routing protocol. Options are:

- rip1 — Accepts RIP version 1 packets.
- rip2 — Accepts RIP version 2 packets.
- both — Accepts RIP version 1 and 2 packets. This is the default value.

authentication — Specifies whether there is password protection. This option only applies to RIP version 2. Options are:

- pass — Specifies password protection. The password is assigned with the PASSWORD parameter.
- none — Specifies no password protection. This is the default setting.

password — Specifies the password used to authenticate RIP version 2 packets. The password can be up to sixteen alphanumeric characters. The password is case sensitive and can include the hyphen and underscore.

Passwords are sent in plaintext. The AT-S63 Management Software does not support encrypted passwords.

Passwords are not supported in RIP version 1.

poisonreverse — Specifies the status for split horizon and split horizon with poison reverse. The options are:

- yes, on, true — Split horizon with poison reverse is enabled. These values are equivalent.
- no, off, false — Split horizon with poison reverse is disabled, and split horizon is executed. This is the default setting. These values are equivalent.

autosummary — Specifies the status of autosummary of routes. The options are:

- yes, on, true — Activates autosummarization of routes. These values are equivalent.
- no, off, false — Disables autosummarization. This is the default setting. These values are equivalent.

Description

This command adds RIP to an interface. It also controls the type of RIP packets sent to and accepted by the interface.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Examples

This command adds RIP to the VLAN5-0 interface and configures the routing protocol to send and accept only version 1 packets. No password is specified since RIP version 1 does not support passwords.

```
add ip rip interface=vlan5-0 send=rip1 receive=rip1
```

This command adds RIP to the VLAN10-0 interface and configures the routing protocol to send version 2 packets and accept packets of either version. Password protection is not used:

```
add ip rip interface=vlan10-0 send=rip2 receive=both
authentication=none
```

This command adds RIP to the VLAN12-2 interface. It configures the protocol to send version 2 packets and accept packets of either version. The password for authentication is “net25aqy”:

```
add ip rip interface=vlan12-2 send=rip2 receive=both
authentication=pass password=net25aqy
```

AlliedWare Plus Command

Syntax

To add RIP to a routing interface:

network *interface*

To set the version of RIP packets the routing protocol will transmit:

send rip1|rip2 *interface*

To set the version of RIP packets the routing protocol will accept:

recv rip1|rip2|both *interface*

To enable or disable password protection for RIP version 2:

authentication pass|none *interface*

To set the password used to authenticate RIP version 2 packets:

password *password interface*

To activate split horizon with poison reverse:

poison-reverse *interface*

To activate split horizon:

no poison-reverse *interface*

To enable autosummary of routes:

auto-summary *interface*

To disable autosummary of routes:

no auto-summary *interface*

Mode

Router mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example adds RIP to the VLAN2-0 interface and configures the routing protocol to send and accept only version 1 packets.

```
awplus> enable
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# network vlan2-0
awplus(config-router)# send rip1 vlan2-0
awplus(config-router)# recv rip1 vlan2-0
```

This example adds RIP to the VLAN4-1 interface and configures the routing protocol to send version 2 packets and to accept both version 1 and version 2 packets. Password authentication is activated for the version 2 packets and the password is set to “atwat225”:

```
awplus> enable
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# network vlan4-1
awplus(config-router)# send rip2 vlan4-1
awplus(config-router)# recv both vlan4-1
awplus(config-router)# authentication pass vlan4-1
awplus(config-router)# password atwat225 vlan4-1
```

ADD IP ROUTE

AlliedWare Plus
Command
Available

Syntax

```
add ip route=ipaddress [interface=interface]
nexthop=ipaddress [mask=subnetmask] [metric=value]
[preference=value]
```

Parameters

route — Specifies the IP address of the destination network, subnet, or node. The IP address for a default route is 0.0.0.0.

interface — Specifies the name of the routing interface where the static route is to be added. To view the interfaces on the switch, refer to "SHOW IP INTERFACE" on page 745.

This parameter is optional. The switch automatically determines the appropriate interface by adding a route to the interface whose IP address is a member of the same subnet as the next hop. (An error message is displayed if you try to add a route to an interface whose IP address is a member of a different subnet than the next hop in the route.)

nexthop — Specifies the IP address of the next hop for the route. The next hop's IP address must be a member of a local subnet on the switch and the subnet must have an interface.

mask — Specifies the subnet mask of the destination IP address of the static route. The default value is based of the address' network type. The default values are:

Class A address - 255.0.0.0

Class B address - 255.255.0.0

Class C address - 255.255.255.0

Do not include a mask for the default route.

Note
In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the "1" bits are consecutive (e.g.,128, 192, 224, etc.).

metric — Specifies the cost of crossing the route. The range is 1 to 16. The default is 1.

preference — Assigns a preference value to the static route. The switch uses the preference values to select the active routes when there are more than eight static or dynamic routes in the routing table to the same remote destination. The range is 0 to 65535. The lower the value, the higher the preference. The default value for a static route is 60. The default value for the default route is 360.

Description

This command is used to create new static routes and a default route on AT-9400 Switches that support IPv4 packet routing.

The only route you can define on AT-9400 Switches that do not support IPv4 packet routing is a default route. The default route specifies the switch’s default gateway. You cannot create any static routes. The management software uses the default route to communicate with other network devices, such as syslog and RADIUS servers, on remote subnets when performing management functions.

Examples

This command adds a static route to a remote subnet with the IP address 149.124.55.0 and a mask of 255.255.255.0. The IP address of the next hop is 149.111.12.4. Specifying an interface is unnecessary because the management software automatically adds the route to the interface that is a member of the same subnet as the next hop:

```
add ip route=149.124.55.0 nexthop=149.111.12.4
mask=255.255.255.0
```

This command adds a static route to a remote subnet with the IP address 149.14.150.0 and the mask 255.255.224.0. The IP address of the next hop is 162.76.44.12. The metric for the route is 5 and the preference is 25:

```
add ip route=162.14.150.0 nexthop=162.76.44.12
mask=255.255.224.0 metric=5 preference=25
```

This command adds a default route. The IP address of the next hop is 172.211.16.12. No mask is specified for a default route. As with a static route, specifying an interface for the default route is unnecessary since the switch automatically adds the route to the interface on the same subnet as the next hop:

```
add ip route=0.0.0.0 nexthop=172.211.16.12
```

AlliedWare Plus Command

Syntax

To create a static route:

```
ip route destination_ip_address/mask nexthop_ip_address
```

To create a default route:

```
ip route 0.0.0.0 nexthop_ip_address
```

Mode

Configure mode

Description

This command does not allow you to specify metric values or preference values for static routes. The default values are used instead.

Examples

This command adds a static route to a remote subnet with the IP address 176.14.145.0 and a mask of 255.255.255.0. The IP address of the next hop is 112.41.12.11:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip route 176.14.145.0/24 112.41.12.11
```

This example creates a default route with the next hop as 171,22,125,8:

```
awplus> enable
awplus# configure terminal
awplus(config)# ip route 0.0.0.0/0 171.22.125.8
```

DELETE IP ARP

AlliedWare Plus Command Available

Syntax

```
delete ip arp=ipaddress
```

Parameters

arp	Specifies the IP address of the host to be deleted from the ARP cache.

Description

This command deletes static and dynamic ARP entries from the ARP cache. This command can delete only one ARP entry at a time. To view the entries in the cache, refer to “SHOW IP ARP” on page 741.

The AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP Switches do not support this command.

Example

This command deletes the ARP entry for a host with the IP address 149.42.67.8:

```
delete ip arp=149.42.67.8
```

AlliedWare Plus Command

Syntax

```
no arp ipaddress
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Examples

This example deletes the ARP entry for the IP address 149.76.32.2:

```
awplus> enable
awplus# configure terminal
awplus(config)# no arp 149.76.32.2
```

This example deletes the ARP entry for the IP address 149.181.37.17:

```
awplus> enable
awplus# configure terminal
awplus(config)# no arp 149.181.37.17
```

DELETE IP INTERFACE

AlliedWare Plus
Command
Available

Syntax

```
delete ip interface=interface
```

Parameters

interface

Specifies the name of the interface to be deleted from the switch. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

Description

This command is used to delete routing interfaces. You can only delete one interface at a time. To display the names of the interfaces, refer to “SHOW IP INTERFACE” on page 745.

Note the following before performing this command:

- All IPv4 packet routing to the local network or subnet of a deleted interface ceases.
- All static routes assigned to the interface are deleted from the route table.
- Deleting an interface used by the AT-S63 Management Software to access a network management device (e.g., a RADIUS or syslog server) causes the switch to stop performing the management function.
- Deleting the local interface on a master switch of an enhanced stack disables the device’s ability to function as the master switch.
- Deleting the local interface of a switch during a remote Telnet or SSH management session immediately ends the session if you accessed the switch directly (i.e., not through enhanced stacking). To continue managing the switch, you must start a local management session using the Terminal Port on the unit.

Examples

This command deletes the VLAN6-2 interface from the switch:

```
delete ip interface=vlan6-2
```

This command deletes an interface using the name of the VLAN, in this case Sales, instead of the VID:

```
delete ip interface=vlan-Sales-2
```

AlliedWare Plus Command

Syntax

```
interface Default_VLAN
no ip address
```

Mode

VLAN Interface mode

Description

This command can only be used to delete the VLAN1-0 interface in the Default VLAN. To delete any other interfaces in the Default VLAN or in any other VLAN,. use the standard command.

Example

This example deletes the VLAN1-0 routing interface from the Default_VLAN:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface Default_VLAN
awplus(config-if)# no ip address
```

DELETE IP RIP

AlliedWare Plus
Command
Available

Syntax

```
delete ip rip interface=interface
```

Parameters

interface — Specifies the name of the interface where RIP is to be removed. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

Description

This command removes RIP from interfaces, which stops the interfaces from routing packets with RIP. However, interfaces, even without RIP, can route packets to other interfaces on the same switch and to remote networks and subnets using static routes.

To view the names of the interfaces using RIP, refer to “SHOW IP RIP COUNTER” on page 747.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Example

This command removes RIP from the VLAN8-0 interface:

```
delete ip rip interface=vlan8-0
```

AlliedWare Plus Command

Syntax

```
no network interface
```

Mode

Router mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Examples

This example removes RIP from the VLAN2-0 interface:

```
awplus> enable
awplus# configure terminal
```

```
awplus(config)# router rip
awplus(config-router)# no network vlan2-0
```

This example removes RIP from the VLAN5-2 interface:

```
awplus> enable
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# no network vlan5-2
```

DELETE IP ROUTE

AlliedWare Plus
Command
Available

Syntax

```
delete ip route=ipaddress [interface=interface]
nexthop=ipaddress mask=subnetmask
```

Parameters

route
Specifies the destination IP address of the static, dynamic, or default route to be deleted. The IP address for the default route is 0.0.0.0.

interface
Specifies the name of the interface where the static or dynamic route is assigned. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). This parameter is optional.

nexthop
Specifies the IP address of the next hop of the route. The next hop is required when deleting a static or dynamic route, but not when deleting a default route.

mask
Specifies the subnet mask for the destination IP address. The mask for the default route is 255.255.255.255.

Description

This command deletes static, dynamic, and default routes from the routing table. To display the current routes, refer to “SHOW IP ROUTE” on page 752.

Examples

This command deletes the static route to the remote subnet 149.124.55.0. The subnet mask is 255.255.255.0 and the next hop is 149.124.22.12

```
delete ip route=149.124.55.0 mask=255.255.255.0
nexthop=149.124.22.12
```

This command deletes a default route that has a next hop of 149.88.62.14:

```
delete ip route=0.0.0.0 nexthop=149.88.62.14 mask=0.0.0.0
```

AlliedWare Plus Command

Syntax

To delete a static route:

```
no ip route destination_ip_address/mask nexthop_ip_address
```

To delete the default route:

```
no ip route 0.0.0.0/0 nexthop_ip_address
```

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This command deletes the static route to the remote subnet 172.23.144.0. The subnet mask is 255.255.255.0 and the next hop is 168.121.87.22

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip route 172.23.144.0/24 168.121.87.22
```

This example creates a default route with the next hop as 171,22,125,8:

```
awplus> enable
awplus# configure terminal
awplus(config)# no ip route 0.0.0.0 171.22.125.8
```

DISABLE IP ROUTE MULTIPATH

Syntax

```
disable ip route multipath
```

Parameters

None.

Description

This command disables the ECMP feature. When the feature is disabled, the routing table in the switch will route packets to a specific remote destination using only one route even in cases where the table contains multiple static or dynamic routes to the destination. Additional routes to the same destination are placed in a standby mode. The default setting for ECMP is enabled. To view the current status of ECMP on the switch, use the SHOW IP ROUTE command with the GENERAL parameter. For instructions, refer to “SHOW IP ROUTE” on page 752.

Example

The following example disables ECMP on the switch:

```
disable ip route multipath
```

ENABLE IP ROUTE MULTIPATH

Syntax

```
enable ip route multipath
```

Parameters

None.

Description

This command enables the ECMP feature. When this feature is enabled, the routing table in the switch routes packets to a specific remote destination using more than one route when the table contains multiple static or dynamic routes to the destination. The table can contain up to 32 routes to the same destination and up to eight of the routes can be active at one time. The default setting for ECMP is enabled. To view the current status of ECMP on the switch, use the SHOW IP ROUTE command with the GENERAL parameter. For instructions, refer to "SHOW IP ROUTE" on page 752.

Example

The following example enables ECMP on the switch:

```
enable ip route multipath
```

PURGE IP

Syntax

```
purge ip
```

Parameters

None.

Description

This command deletes all routing interfaces on the switch. Note the following before performing this command:

- ❐ All IPv4 packet routing on the switch ceases. The device, however, continues to switch packets among the ports within the VLANs (but not across the VLAN boundaries) using Layer 2.
- ❐ All static routes are deleted from the route table.
- ❐ The AT-S63 Management Software stops performing those management functions that require access to a network management device (e.g., a RADIUS server).
- ❐ Deleting all interfaces deletes the local interface. This prohibits you from remotely managing the device with a Telnet or SSH client, or with a web browser.
- ❐ Deleting all interfaces during a remote Telnet or SSH management session immediately ends your session. To continue managing the switch, you must start a local management session using the Terminal Port on the unit.
- ❐ Deleting all interfaces on the master switch of an enhanced stack disables the device’s ability to function as the master switch of the stack.

Example

This command deletes all routing interfaces on the switch:

```
purge ip interface
```

SET IP ARP

Syntax

```
set ip arp=ipaddress [interface=interface] [port=port]
[ethernet=macaddress]
```

Parameters

arp	Specifies the IP address of the static route entry to be modified.
interface	Specifies the interface where the host is located. An interface name consists of "VLAN" followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). The interface must already exist on the switch.
port	Specifies a new physical port on the switch where the host is located.
ethernet	Specifies a new MAC address of the host. The MAC address can be entered in either of the following formats: xxxxxxxxxxxx or xx:xx:xx:xx:xx:xx

Description

This command modifies an existing static ARP entry in the ARP cache. You can change all of the settings of an entry, except the IP address. To change the IP address, you must delete the entry and add it again. To view the ARP entries, refer to "SHOW IP ARP" on page 741.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Examples

This command modifies the port number for the static ARP entry with the IP address 149.42.67.8:

```
set ip arp=149.42.67.8 port=24
```

This command changes the MAC address for the static ARP entry with the IP address 149.124.85.14:

```
set ip arp=149.124.85.14 ethernet=00:06:7a:22:11:24
```

SET IP ARP TIMEOUT

Syntax

```
set ip arp timeout=integer
```

Parameter

timeout	Specifies the ARP cache timeout value The range is 150 to 260000 seconds. The default setting is 600 seconds.

Description

This command sets the ARP cache timeout value. The timer prevents the ARP table from becoming full with inactive entries. An entry that is not used for the length of the timeout period is designated as inactive and deleted from the table. To view the current timeout value, refer to “SHOW IP ARP” on page 741.

Example

The following command sets the timer to 400 seconds:

```
set ip arp timeout=400
```

SET IP INTERFACE

Syntax

```
set ip interface=interface|eth0
[ipaddress=ipaddress|dhcp|bootp] [mask|netmask=subnetmask]
[ripmetric=value]
```

Parameters

interface — Specifies the name of the routing interface to be modified. An interface name consists of "VLAN" followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). The "eth0" value can be used in place of the interface name to specify the local interface.

ipaddress — Specifies a new IP address for the interface.

mask **or** netmask — Specifies a new subnet mask for the interface. Do not specify a mask if the IP address is assigned by a DHCP or BOOTP server. To change the subnet mask, you must also include the IP address of the interface. The default value is based on the address' network type. The default values are:

Class A address - 255.0.0.0

Class B address - 255.255.0.0

Class C address - 255.255.255.0

Note
In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the "1" bits are consecutive (e.g.,128, 192, 224, etc.).

ripmetric — Specifies the new cost of crossing the interface for RIP. The range is 1 to 16. The default is 1.

Description

This command modifies the IP address, subnet mask and RIP metric attribute of an existing routing interface. To initially create an interface, refer to "ADD IP INTERFACE" on page 708. To view the interfaces, refer to "SHOW IP INTERFACE" on page 745

Note the following before performing this command:

- Modifying the IP address of a routing interface deletes all static routes assigned to the interface.
- Modifying the IP address of a routing interface that has RIP removes the routing protocol from the interface and deletes all RIP routes learned on the interface from the routing table.
- You cannot change the name of a routing interface. You must delete the interface and recreate it to change its VID or interface number.
- You can specify the local interface two ways. You can specify its interface name (for example, VLAN5-1) or use the “eth0” value. The “0” in the value is not a VID, as in an interface name. Rather, the “eth0” value signifies the local interface. To designate the local interface of a switch, refer to “SET IP LOCAL INTERFACE” on page 733.

Examples

This command changes the IP address of the VLAN7-0 interface to 149.188.27.55 and the subnet mask to 255.255.255.0:

```
set ip interface=vlan7-0 ipaddress=149.188.27.55
mask=255.255.255.0
```

This command activates the DHCP client on the VLAN 28-5 interface so that it obtain its IP address and subnet mask from a DHCP server:

```
set ip interface=vlan28-5 ipaddress=dhcp
```

This command changes the RIP metric for the VLAN12-0 interface to 2:

```
set ip interface=vlan12-0 ripmetric=2
```

This command changes the IP address and subnet mask of the local interface to 149.24.252.6 and 255.255.240.0, respectively. The example uses “eth0” rather than the interface name to designate the local interface:

```
set ip interface=eth0 ipaddress=149.24.252.6
mask=255.255.240.0
```

SET IP LOCAL INTERFACE

AlliedWare Plus Command Available

Syntax

```
set ip local interface=interface|none
```

Parameters

interface

Specifies the name of the interface to act as the local interface on the switch. An interface name consists of "VLAN" followed by the name or the ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

Use the NONE option to remove the currently assigned local interface without assigning a new one. The default is no local interface.

Description

This command specifies the local interface of the switch. The selected interface must already exist on the switch. The local interface is used for enhanced stacking and for remote management of the unit with a Telnet or SSH client, or a web browser. A switch can have only one local interface at a time. To view the interfaces on the switch, refer to "SHOW IP INTERFACE" on page 745.

Examples

This command specifies the VLAN6-0 interface as the local interface on the switch:

```
set ip local interface=vlan6-0
```

This command specifies the interface with the interface number 2 in the Sales VLAN as the local interface on the switch:

```
set ip local interface=vlan-Sales-2
```

This command removes the currently assigned local interface without assigning a new one:

```
set ip local interface=none
```

AlliedWare Plus Command

Syntax

```
interface Default_VLAN
ifconfig eth0
```

Mode

VLAN Interface mode

Description

This command can only be used to designate the VLAN1-0 interface in the Default VLAN as the local interface. To designate another interface as the local interface, use the standard command.

Example

This example designates the VLAN1-0 interface in the Default VLAN as the local interface:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface Default_VLAN
awplus(config-if)# ifconfig eth0
```

SET IP RIP

AlliedWare Plus Command Available

Syntax

```
set ip rip interface=interface [send=rip1|rip2]
[receive=rip1|rip2|both] [authentication=pass|none]
[password=password]
[poisonreverse=yes|no|on|off|true|false]
[autosummary=yes|no|on|off|true|false]
```

Parameters

interface — Specifies the name of an interface whose RIP settings are to be modified. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

send — Specifies the version of the RIP packets to be sent by the interface. Options are:

- rip1 — Sends RIP version 1 packets. This is the default value.
- rip2 — Sends RIP version 2 packets.

receive — Specifies the version of the RIP packets to be accepted by the interface. Options are:

- rip1 — Accepts RIP version 1 packets.
- rip2 — Accepts RIP version 2 packets.
- both — Accepts RIP version 1 and 2 packets. This is the default value.

authentication — Specifies whether there is password protection. This option only applies to RIP version 2. Options are:

- pass — Specifies password protection. The password is specified with the PASSWORD parameter.
- none — Specifies no password protection. This is the default setting.

password — Specifies the password used to authenticate RIP version 2 packets. The password can be up to sixteen alphanumeric characters. The password is case sensitive and can include the hyphen and underscore.

The interface must be configured for RIP version 2 in order for you to specify a password. Passwords are not supported in RIP version 1.

Passwords are sent in plaintext. The AT-S63 Management Software does not support encrypted passwords.

poisonreverse Specifies the status for split horizon and split horizon with poison reverse. The options are:

yes, on, true Split horizon poison reverse is enabled. These values are equivalent.

no, off, false Split horizon poison reverse is disabled, and split horizon is executed. This is the default setting. These values are equivalent.

autosummary Specifies the status for autosummarization of routes. The options are:

yes, on, true Autosummarization of routes on the RIP interface is enabled. These values are equivalent.

no, off, false Autosummarization of routes on the RIP interface is disabled. This is the default setting. These values are equivalent.

Description

This command modifies the RIP settings of an interface. To initially add RIP to an interface, refer to “ADD IP RIP” on page 711. To view the interfaces on the switch, refer to “SHOW IP INTERFACE” on page 745.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Examples

This command changes RIP on the VLAN4-3 interface to send version 2 packets, accept either version 1 or 2, and use the password “wa24pt” for authentication:

```
set ip rip interface=vlan4-3 send=rip2 receive=both
authentication=pass password=wa24pt
```

This command changes RIP on the VLAN11-0 interface to accept both RIP version 1 and version 2 packets:

```
set ip rip interface=vlan11-0 receive=both
```

This command changes RIP on the VLAN22-1 interface to send and receive RIP version 1 packets. Since version 1 does not support password authentication, the command disables it:

```
set ip rip interface=vlan22-1 send=rip1 receive=rip1
authentication=none
```

Note
Password authentication must be disabled to change an interface from RIP version 2 to version 1.

AlliedWare Plus Command

Syntax

To set the version of RIP packets the routing protocol will transmit:

```
send rip1|rip2 interface
```

To set the version of RIP packets the routing protocol will accept:

```
recv rip1|rip2|both interface
```

To enable or disable password protection for RIP version 2:

```
authentication pass|none interface
```

To set the password used to authenticate RIP version 2 packets:

```
password password interface
```

To activate split horizon with poison reverse:

```
poison-reverse interface
```

To activate split horizon:

```
no poison-reverse interface
```

To enable autosummary of routes:

```
auto-summary interface
```

To disable autosummary of routes:

```
no auto-summary interface
```

Mode

Router mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example changes the settings for RIP on the VLAN2-0 interface. It configures the routing protocol to send and accept only version 2 packets. Password authentication is activated and the password is set to “ba124”:

```
awplus> enable
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# send rip2 vlan2-0
awplus(config-router)# recv rip2 vlan2-0
awplus(config-router)# authentication pass vlan2-0
awplus(config-router)# password ba124 vlan2-0
```

This example changes the RIP settings on the VLAN4-1 interface. It configures the routing protocol to send version 2 packets and to accept both version 1 and version 2 packets, without password authentication:

```
awplus> enable
awplus# configure terminal
awplus(config)# router rip
awplus(config-router)# send rip2 vlan4-1
awplus(config-router)# recv both vlan4-1
awplus(config-router)# authentication none vlan4-1
```

SET IP ROUTE

Syntax

```
set ip route=ipaddress [interface=interface]
nexthop=ipaddress mask=subnetmask [metric=value]
[preference=value]
```

Parameters

route

Specifies the IP address of the remote destination of the static route to be modified. The IP address of the default route is 0.0.0.0.

You cannot change the destination IP address of a static route. If the destination address changes, you must delete the old route and enter a new route.

interface

Specifies the name of the interface where the next hop is located. To view the interfaces on the switch, refer to "SHOW IP INTERFACE" on page 745.

Allied Telesis recommends omitting this optional parameter. The appropriate interface for a static route is determined automatically by the switch when it examines the IP address of the next hop and adds the route to the interface of the same subnet.

nexthop

Specifies the IP address of the next hop of the route. You must specify the next hop even if you are not changing it.

If the IP address of the next hop belongs to a different subnet than the original IP address, the switch automatically moves the route to the appropriate interface.

mask

Specifies the subnet mask for the destination IP address. The default value is based of the address' network type. The default values are:

Class A address - 255.0.0.0

Class B address - 255.255.0.0

Class C address - 255.255.255.0

Do not include a mask for a default route.

Note
In version 2.0.0, the routing table supported only these three values for subnet masks. In all later versions, subnet masks can be of variable lengths, provided that the “1” bits are consecutive (e.g.,128, 192, 224, etc.).

metric	Specifies a new cost for crossing the route. The range is 1 to 16. The default is 1.
preference	Assigns a preference value to the static route. The switch uses the preference values to select the active routes when there are more than eight static or dynamic routes in the routing table to the same remote destination. The range is 0 to 65535. The lower the value, the higher the preference. The default value for a static route is 60. The default value for the default route is 360.

Description

This command modifies the attributes of an existing static route or default route. You can use the command to change the IP address of the next hop or the subnet mask of the destination address. The command can also change the metric cost of a route. This command cannot change the destination address. Changing the destination address requires deleting a static route and recreating it with the new address. To view the static routes, refer to “SHOW IP ROUTE” on page 752.

Examples

This command changes the IP address of the next hop for the static route to the remote subnet 149.124.55.0. The IP address of the next hop is changed to 149.124.52.4:

```
set ip route=149.124.55.0 nexthop=149.124.52.4
mask=255.255.255.0
```

This command changes the metric value to 7 for the static route to the remote subnet 172.55.156.0:

```
set ip route=172.55.156.0 nexthop=172.55.101.2
mask=255.255.255.0 metric=7
```

This command changes the IP address of the next hop to 149.211.16.12 for the default route:

```
set ip route=0.0.0.0 nexthop=149.211.16.12
```

SHOW IP ARP

AlliedWare Plus
Command
Available

Syntax

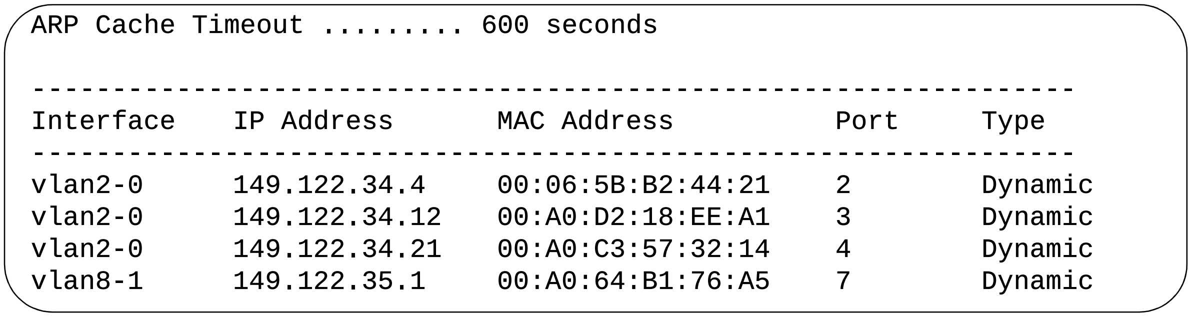
```
show ip arp
```

Parameters

None.

Description

This command displays the entries in the ARP cache. The ARP cache contains mappings of IP addresses to physical addresses for hosts where the switch has recently routed packets. Figure 80 is an example of the information displayed by this command.



```
ARP Cache Timeout ......... 600 seconds

-----------------------------------------------------------------
Interface    IP Address      MAC Address          Port     Type
-----------------------------------------------------------------
vlan2-0      149.122.34.4    00:06:5B:B2:44:21    2        Dynamic
vlan2-0      149.122.34.12   00:A0:D2:18:EE:A1    3        Dynamic
vlan2-0      149.122.34.21   00:A0:C3:57:32:14    4        Dynamic
vlan8-1      149.122.35.1    00:A0:64:B1:76:A5    7        Dynamic
```

Figure 80. SHOW IP ARP Command

The columns in the display are:

- Interface - Interface from where the network device is accessed.
- IP Address - IP address of the node.
- MAC Address - MAC address of the node.
- Port - Port on the switch from where the node is accessed.
- Type - Type of entry. This is one of the following:
  - Static: Static entry added with "ADD IP ARP" on page 706.
  - Dynamic: Entry learned from ARP request/reply exchanges.
  - Invalid: Possible nonexistent entry.
  - Other: Entry automatically generated by the system.

To set the ARP timeout value, refer to "SET IP ARP TIMEOUT" on page 730.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Example

This command displays the entries in the ARP cache:

```
show ip arp
```

AlliedWare Plus Command

Syntax

```
show arp
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show arp
```

SHOW IP COUNTER

Syntax

```
show ip counter [port=ports|all]
```

Parameters

port Specifies the ports whose IP statistics you want to display. For instructions on how to enter port numbers, refer to "Port Numbers in Commands" on page 48. Omitting this parameter displays the statistics for all the ports.

Description

This command displays Layer 3 counters for the individual ports on a switch. Figure 81 is an example of the information displayed by this command.

```
Port 1

IPInUcastPkts ................... 0
IPOutUcastPkts .................. 0
IPInDiscards .................... 0
IPInHdrErrors ................... 0


Port 2

IPInUcastPkts ................... 0
IPOutUcastPkts .................. 0
IPInDiscards .................... 0
IPInHdrErrors ................... 0
```

Figure 81. SHOW IP COUNTER Command

The lines in the display are:

- IPInUcastPkts - Number of IP packets received on a port.
- IPOutUcastPkts - Number of IP packets transmitted from a port.
- IPInDiscards - Number of IP packets received but discarded due to resource limitations at the IP level.
- IPInHdrErrors - Number of IP packets received with header errors.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Examples

This command displays the statistics for all the ports:

```
show ip counter
```

This command displays the statistics for ports 1 to 4:

```
show ip counter port=1-4
```

SHOW IP INTERFACE

AlliedWare Plus
Command
Available

Syntax

```
show ip interface[=interface|eth0]
```

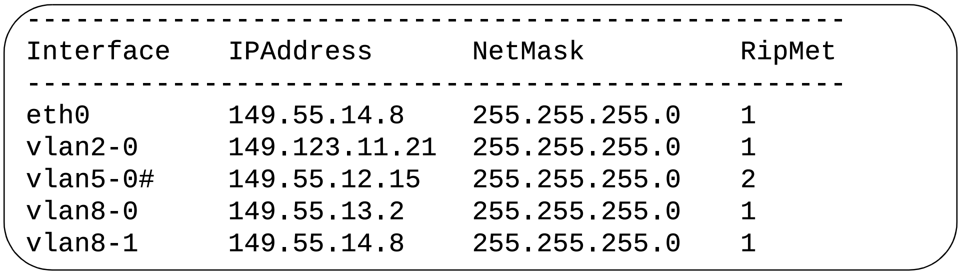
Parameters

interface — Specifies the interface name. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0). If no interface value is specified, the switch displays all the interfaces.

The “eth0” value can be used to designate the local interface.

Description

This command displays the routing interfaces on a switch. An example of the information displayed by this command is shown in Figure 82.



```
---------------------------------------------------
Interface    IPAddress      NetMask         RipMet
---------------------------------------------------
eth0         149.55.14.8    255.255.255.0    1
vlan2-0      149.123.11.21  255.255.255.0    1
vlan5-0#     149.55.12.15   255.255.255.0    2
vlan8-0      149.55.13.2    255.255.255.0    1
vlan8-1      149.55.14.8    255.255.255.0    1
```

Figure 82. SHOW IP INTERFACE Command

The local interface of a switch, if one has been designated, is listed twice in the table, as “eth0” at the top of the table and again as a regular entry. For instance, the local interface on the switch in the above example is the VLAN8-1 interface because its values and those of the “eth0” interface are identical. The “eth0” entry contains null values (i.e., 0.0.0.0) if no local interface is designated on the unit.

The columns in the display are:

- Interface - The interface name consisting of the VLAN’s identification (VID) and interface number. A hash symbol (#) marks IP interfaces where there are no active nodes in the VLAN on the switch.
- IPAddress - The interface’s IP address. The address is assigned manually to the interface or automatically by a DHCP or BOOTP server. If the address is 0.0.0.0, the interface is configured to receive

its IP configuration from a DHCP or BOOTP server, but the server has not responded.

- NetMask - The interface’s subnet mask. The subnet mask is assigned manually to the interface or automatically by a DHCP or BOOTP server. If the mask is 0.0.0.0, the DHCP or BOOTP server has not responded.
- RipMet - The hop count for this interface when routing packets with RIP.

Examples

This command displays all the routing interfaces on a switch:

```
show ip interface
```

This command displays just the VLAN2-6 interface:

```
show ip interface=vlan2-6
```

AlliedWare Plus Command

Syntax

```
show ip interface brief
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

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

SHOW IP RIP COUNTER

Syntax

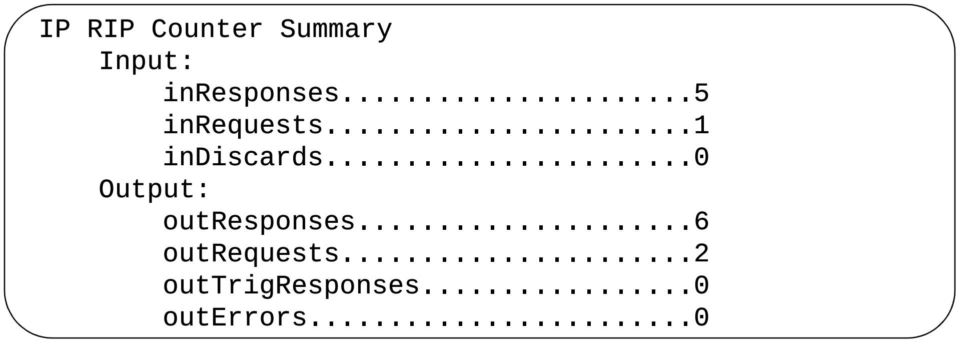
```
show ip rip counter
```

Parameters

counter	Displays RIP packet statistics for all interfaces where RIP has been added. This parameter cannot be used with the INTERFACE parameter.

Description

This command displays RIP statistics for the entire switch. An example of the information displayed by this command is shown in Figure 83.



```
IP RIP Counter Summary
    Input:
        inResponses.....................5
        inRequests......................1
        inDiscards......................0
    Output:
        outResponses....................6
        outRequests.....................2
        outTrigResponses................0
        outErrors.......................0
```

Figure 83. SHOW IP RIP Command with COUNTER Parameter

The columns in the display are described here:

- inResponse - The number of response packets received.
- inRequests - The number of request packets received.
- inDiscards - The number of packets discarded. Packets may be discarded due to an authentication failure or a mismatched sequence number of a triggered acknowledgement.
- outResponse - The number of response packets sent.
- outRequests - The number of request packets sent.
- outTrigResponse - The number of triggered response packets sent.
- outErrors - The number of errors encountered when sending a request or response RIP message.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP switches.

Example

This command displays RIP packet statistics:

```
show ip rip counter
```

SHOW IP RIP INTERFACE

AlliedWare Plus
Command
Available

Syntax

```
show ip rip interface[=interface]
```

Parameters

interface — Specifies the interface name. An interface name consists of “VLAN” and the ID (VID) followed by the VLAN name or interface number, separated by a dash (e.g., vlan4-Sales or vlan4-0). If no interface value is specified, the switch displays all the interfaces with the routing protocol.

Description

This command lists the RIP settings on those routing interfaces that have RIP. An example of the information displayed by this command is shown in Figure 84.

```
----------------------------------------------------------------------------
Interface      Send  Recv     Auth   Password   PoisonReverse    AutoSummary
----------------------------------------------------------------------------
vlan2-0        RIP2  BOTH     PASS   ********   On               On
vlan5-0        RIP1  BOTH     NONE   NOT SET    Off              On
vlan8-0        RIP2  BOTH     PASS   ********   Off              Off
vlan8-1        RIP2  BOTH     PASS   ********   On               On
```

Figure 84. SHOW IP RIP Command

The columns in the display are described here:

- Interface - An interface name consisting of a VLAN’s identification (VID) number and interface number.
- Send - The version of RIP packets sent by the interface. Possible settings are:
  - RIP1: version 1 packets
  - RIP2: version 2 packets
- Receive - The version of RIP packets the interface will accept. Possible settings are:
  - RIP1: version 1 packets
  - RIP2: version 2 packets
  - BOTH: both version 1 and 2 packets

- Auth - The form of authentication. Possible settings are:
  - NONE: no password authentication
  - PASS: plaintext password authentication
- Password - The authentication password, displayed with asterisks. A value of NOT SET in this column indicates the interface does not have a password for RIP.
- PoisonReverse - The status of split horizon and split horizon with poison reverse:
  - OFF: The interface is using split horizon only. This is the default setting.
  - ON: The interface is using split horizon with poison reverse.
- AutoSummary - The status of route autosummarization:
  - OFF: The interface is not using route autosummarization. This is the default setting.
  - ON: The interface is using autosummarization.

To add RIP to an interface, refer to “ADD IP RIP” on page 711. To modify the RIP settings of an interface, refer to “SET IP RIP” on page 735.

This command is not available on the AT-9408LC/SP, AT-9424T/GB, and AT-9424T/SP Switches.

Examples

This command displays the RIP settings for all the interfaces that have the routing protocol:

```
show ip rip interface
```

This command displays the RIP settings for the VLAN17-2 interface:

```
show ip rip interface=vlan17-2
```

The command does not display anything if the VLAN17-2 interface does not have RIP.

AlliedWare Plus Command

Syntax

```
show router-rip [interface]
```

Modes

User Exec mode and Privileged Exec mode

Description

This command is equivalent to the standard command.

Example

```
awplus# show router-rip
```

SHOW IP ROUTE

AlliedWare Plus Command Available

Syntax

```
show ip route [general] [fdb] [full]
```

Parameters

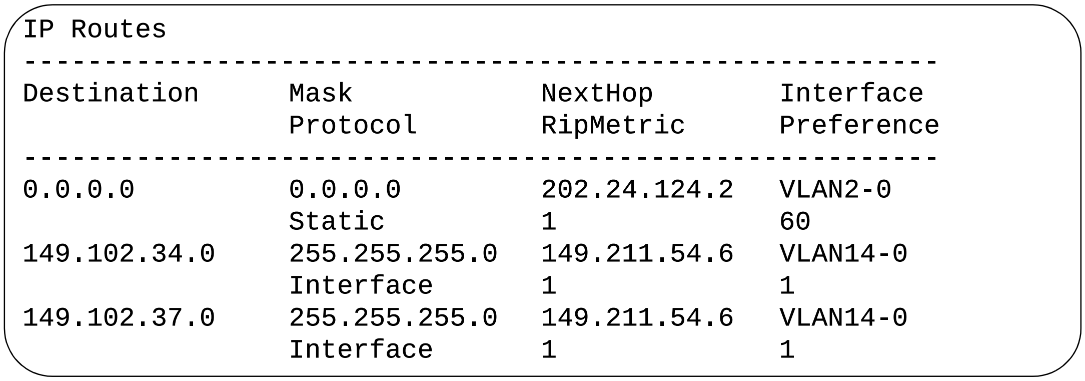
general
: Displays general routing information, such as the total number of routes in the cache and the cache size.

fdb
: Displays the status of the static and dynamic routes.

full
: Displays both the routes and the general routing information.

Description

Entering this command without the optional parameters displays all the static and RIP routes on the IPv4 interfaces. An example of the information is shown in Figure 85.



```
IP Routes
---------------------------------------------------------
Destination      Mask             NextHop         Interface
                 Protocol         RipMetric       Preference
---------------------------------------------------------
0.0.0.0          0.0.0.0          202.24.124.2    VLAN2-0
                 Static           1               60
149.102.34.0     255.255.255.0    149.211.54.6    VLAN14-0
                 Interface        1               1
149.102.37.0     255.255.255.0    149.211.54.6    VLAN14-0
                 Interface        1               1
```

Figure 85. SHOW IP ROUTE Command

The columns are described here:

- Destination - Destination IP address of the network or subnet. The default route is 0.0.0.0.
- Mask - Subnet mask of the destination IP address.
- Protocol - Source of the route. Possible options are:
  - Interface - Route was learned by a routing interface.
  - Static - Route was entered manually as a static route.
  - RIP - Route was learned by RIP.

- NextHop - IP address of the next hop to the destination network or subnet.
- RipMetric - RIP metric (cost) to reaching the destination.
- Interface - Name of the interface where the next hop of the route is located. A hash symbol (#) following the name signifies that the route is physically "down," meaning there are no active nodes in the VLAN of the interface.
- Preference - The preference value of the route. The preference value is used by the switch to select a route when there is more than one route to a remote destination.

Though this command always displays interface and static routes, RIP routes are only displayed when the outgoing interface is up. Note that routes are only propagated by RIP when their status at the physical level is up. This means that a VLAN's interface route is propagated if at least one port in the VLAN is active.

The FDB parameter allows you to view the status of the static and RIP routes on the switch. Figure 86 is an example of the information provided by the FDB parameter.

```
IP FDB
-------------------------------------------------------------
Destination    Mask             NextHop          Interface
Installed      Protocol         RipMetric        Preference
-------------------------------------------------------------
0.0.0.0        255.255.255.0    149.111.44.22    VLAN4-0
Yes            Static           1                60
149.222.66.0   255.255.255.0    149.111.22.11    VLAN2-0
Yes            Static           1                60
149.222.66.0   255.255.255.0    149.111.44.22    VLAN4-0
Yes            Static           1                60
149.222.66.0   255.255.255.0    149.111.55.17    VLAN8-0
Yes            Static           1                60
149.125.10.0   255.255.255.0    149.111.22.11    VLAN2-0
Yes            Static           1                60
```

Figure 86. SHOW IP ROUTE Command with the FDB Parameter

Most of the information displayed by the FDB parameter is identical to that displayed when the command is entered without any parameters. The difference is the addition of the Installed variable which displays the status of the static and RIP routes, and the default route. (The FDB parameter does not display interface routes.) A route with an Installed status of Yes has been installed by the switch in its routing hardware. The route is ready for use (or is already being used) and meets both of the following conditions:

- The interface with the next hop of the route is up (i.e., there is at least one active port in the VLAN)
- There is a static or dynamic ARP entry for the next hop in the routing table.

A route with a status of No has not been installed by the switch in its routing hardware and is not currently being used. Any one of the following conditions can cause a route to have this status:

- The interface for the next hop of the route is down (i.e., there are no active ports in the VLAN)
- The ARP table does not contain a static or dynamic entry for the next hop.
- There are already eight active routes to the same remote destination in the routing table and the route has been placed in the standby mode.

Figure 87 is an example of the information provided by the GENERAL parameter.

```
IP Route General Information
Number of routes................ 25
Interface routes................ 11
RIP routes...................... 12
Static routes................... 2
Cache size...................... 1024
Source route byte counting ..... no
Route debugging................. no
Multipath routing............... yes
```

Figure 87. SHOW IP ROUTE Command with the GENERAL Parameter

The information displayed by the GENERAL parameter is described here:

- Number of routes - Total number of routing interfaces, static routes, and dynamic RIP routes.
- Interface routes - Number of routing interfaces on the switch.
- RIP routes - Number of routes learned by RIP.
- Static routes - Number of static routes.
- Cache size - Size of the route cache (the maximum number of entries)
- Source route byte counting - Whether source route byte counting is enabled.
- Route debugging - Whether route debugging is enabled.
- Multipath routing - Whether ECMP routing is enabled or disabled on the switch. To enable or disable the feature, refer to “ENABLE IP ROUTE MULTIPATH” on page 727 and “DISABLE IP ROUTE MULTIPATH” on page 726.

Examples

This command displays the IPv4 packet routes on the switch:

```
show ip route
```

This command displays general routing information:

```
show ip route general
```

This command displays both the routes and the general routing information:

```
show ip route full
```

AlliedWare Plus Command

Syntax

```
show ip route
```

Modes

User Exec mode and Privileged Exec mode

Description

This command is equivalent to entering the standard SHOW IP ROUTE command without any of the parameters.

Example

```
awplus# show ip route
```

Chapter 39

BOOTP Relay Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter has the following commands:

ADD BOOTP RELAY

Syntax

```
add bootp relay=ipaddress
```

Parameters

ipaddress	Specifies the IP address of a DHCP or BOOTP server.

Description

This command specifies the IP address of a DHCP or BOOTP server. The switch can store up to eight server IP addresses, but you can specify only one at a time with this command.

Example

This example adds the IP address 145.42.19.162 as a DHCP or BOOTP server:

```
add bootp relay=145.42.19.162
```

DELETE BOOTP RELAY

Syntax

```
delete bootp relay=ipaddress
```

Parameters

ipaddress	Specifies the IP address of a DHCP or BOOTP server to be deleted from the switch.

Description

This command deletes the IP address of a DHCP or BOOTP server from the switch. You can delete only one address one at a time with this command.

Example

This example deletes the server IP address 145.42.19.162:

```
delete bootp relay=145.42.19.162
```

DISABLE BOOTP RELAY

Syntax

```
disable bootp relay
```

Parameters

None.

Description

This command deactivates the BOOTP relay agent on the switch. The routing interfaces stop forwarding BOOTP requests to DHCP or BOOTP servers from the clients on the local subnets of the switch.

Example

```
disable boot relay
```

ENABLE BOOTP RELAY

Syntax

```
enable bootp relay
```

Parameters

None.

Description

This command activates the BOOTP relay agent on the switch. The routing interfaces act as relay agents for the clients of the local subnets on the switch.

Example

```
enable boot relay
```

PURGE BOOTP RELAY

Syntax

```
purge bootp relay
```

Parameters

None.

Description

This command deactivates the BOOTP relay agent on the switch and deletes all DHCP and BOOTP server IP addresses.

Example

```
purge boot relay
```

SHOW BOOTP RELAY

Syntax

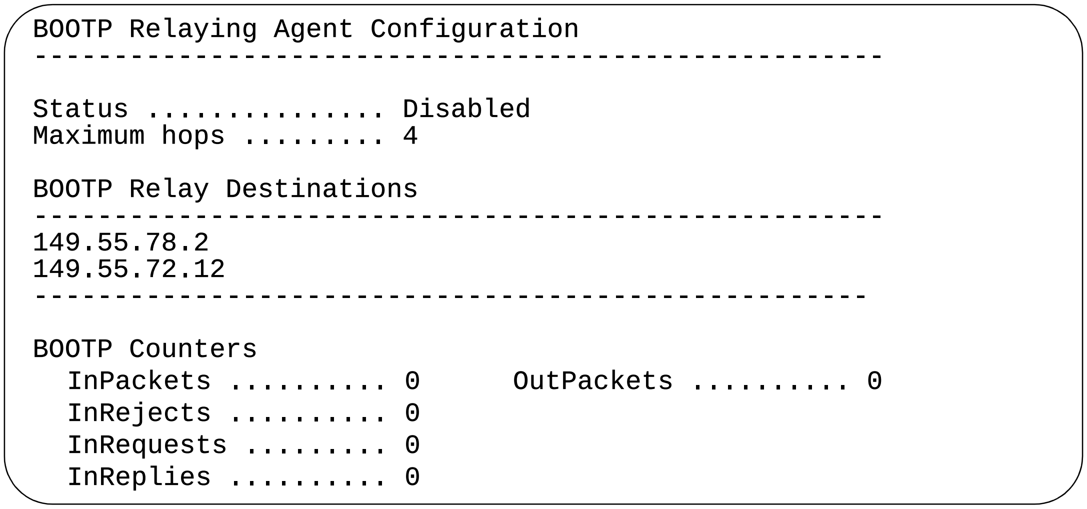
```
show bootp relay
```

Parameters

None.

Description

This command displays the status of the BOOTP relay agent, the IP addresses of the servers, and packet statistics. An example of the display is shown in Figure 88.



```
BOOTP Relaying Agent Configuration
-----------------------------------------------------

Status ............... Disabled
Maximum hops ......... 4

BOOTP Relay Destinations
-----------------------------------------------------
149.55.78.2
149.55.72.12
----------------------------------------------------

BOOTP Counters
  InPackets .......... 0     OutPackets .......... 0
  InRejects .......... 0
  InRequests ......... 0
  InReplies .......... 0
```

Figure 88. SHOW BOOTP RELAY Command

The fields in the display are:

- Status: The agent's status of disabled, the default, or enabled. The routing interfaces do not forward BOOTP requests when the status of the BOOTP relay agent is disabled, and do when the status is enabled. The status is set with "DISABLE BOOTP RELAY" on page 760 and "ENABLE BOOTP RELAY" on page 761.
- Maximum hops: Maximum value allowed for the hops field in a BOOTP message before the message is discarded. The default is 4 hops. This value cannot be changed.
- BOOTP Relay Destinations: The IP addresses of the DHCP or BOOTP servers, set with "ADD BOOTP RELAY" on page 758.

The BOOTP statistics are:

- InPackets: Total number of BOOTP packets received.
- InRejects: Total number of incoming BOOTP packets rejected because of an error in the packet.
- InRequests: Number of BOOTP requests received.
- InReplies: Number of BOOTP replies received.
- OutPackets: Total number of BOOTP packets transmitted.

Example

```
show boot relay
```

Chapter 40

Virtual Router Redundancy Protocol (VRRP) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	
AT-9424T/GB	
AT-9424T/SP	
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter has the following commands:

ADD VRRP IPADDRESS

AlliedWare Plus Command Available

Syntax

```
add vrrp=vrid ipaddress=ipaddress
```

Parameters

vrrp	Specifies the ID of the virtual router, a number between 1 and 255.
ipaddress	Specifies a secondary IP address to be backed up by the specified virtual router. The IP address must be compatible with the IP address and subnet mask associated with the Ethernet interface over which the virtual router is operating.

Description

This command adds a secondary IP address to the group of IP addresses that are backed up by the specified virtual router. The new IP address must be added to all the switches participating in the virtual router. The maximum number of secondary addresses is 16.

Example

This example adds the IP address 205.42.19.162 to the group of IP addresses that are backed up by the virtual router whose VRID is 34:

```
add vrrp=34 ipaddress=205.42.19.162
```

AlliedWare Plus Command

Syntax

```
router vrrp vrid
interface ipaddress
```

Modes

For the ROUTER VRRP command:

Configure mode

For the INTERFACE command:

VRRP mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This example adds the IP address 172.112.45.78 to a virtual router with a VRID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 12
awplus(config-router)# interface 172.112.45.78
```

ADD VRRP MONITOREDINTERFACE

Syntax

```
add vrrp=vrid monitoredinterface=interface
[newpriority=1...254]
```

Parameters

vrrp — Specifies the ID of the virtual router, a number between 1 and 255.

monitoredinterface — Specifies the name of the monitored interface from where the host is reached. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

The interface must already exist. A virtual router can monitor up to 60 interfaces.

newpriority — Specifies the value that is to be used as the switch’s priority if the interface specified by the monitoredinterface parameter becomes inoperative. The range is 1 to 254 and the default is 50.

Description

This command adds a new monitored interface to a virtual router. The monitored interface is the one that the virtual router is dependent upon, usually an interface that provides a WAN link to the switch. This interface must not be the same interface that the virtual router is operating over, as specified in the CREATE VRRP command.

Example

This example adds the VLAN2-2 interface to the group of interfaces monitored by the virtual router with a VRID of 8, with a new priority of 30:

```
add vrrp=8 monitoredinterface=vlan2-2 newpriority=30
```

CREATE VRRP

AlliedWare Plus Command Available

Syntax

```
create vrrp=vrid over=interface ipaddress=ipaddress
[adinterval=1...255] [authentication=none|plaintext]
[password=password] [portmonitoring=on|off]
[portreset=on|off] [preempt=on|off] [priority=1..254]
[stepvalue=1..254|proportional] [delay=0..3600]
```

Parameters

vrrp — Specifies the ID of the virtual router, a number between 1 and 255.

over — Specifies the interface over which the virtual router will send and receive packets. An interface name consists of "VLAN" followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

ipaddress — Specifies a secondary IP address to be backed up by the specified virtual router. The IP address must be compatible with the IP address and subnet mask associated with the Ethernet interface over which the virtual router is operating.

adinterval — Specifies the interval in seconds between advertisement packets. The range is 1 to 255 seconds and the default is 1 second. You must configure all switches in the same virtual router with the same adinterval.

authentication — Specifies whether there is authentication. Options are:

- none — Specifies no authentication. This is the default setting.
- plaintext — Specifies that authentication is required, which you set with the password parameter.

password — Specifies the password used to authenticate VRRP packets. The password can be up to 8 alphanumeric characters. The password is case sensitive and can include the hyphen and underscore.

Passwords are sent in plaintext. The AT-S63 Management Software does not support encrypted passwords.

You must configure all switches in the same virtual router with the same password.

portmonitoring

Specifies whether the VRRP should monitor the ports of the VLAN and alter the priority value if ports fail or are disabled. The options are:

on — Specifies that port monitoring should be on. If you choose not to specify a stepvalue, the stepvalue is set to proportional by default.

off — Specifies that port monitoring should be off. This is the default.

portreset

Specifies that ports of a VLAN that has a virtual router be reset when a virtual router transitions from backup to master status. The options are:

on — Specifies that the VLAN ports be reset.

off — Specifies that the VLAN ports are not reset.

preempt

Specifies whether a higher priority switch preempts a lower priority switch acting as the master. The preferred master (with a priority of 255) always assumes the master role when it is available, regardless of how this parameter is set. The options are:

on — Specifies that preempting should occur. This is the default.

off — Specifies that preempt mode not be used.

You must configure all switches in the same virtual router with the same preempt setting.

priority

Specifies the switch’s priority for becoming the master for the virtual router. The higher the value, the greater the priority. The range is 1 to 254 and the default is 100. The value of 255 is reserved for and assigned to the switch that is the preferred master (the switch owning the virtual router’s IP address), regardless of how this parameter is set.

stepvalue — Specifies the value by which the priority of the virtual router should be decremented each time a VLAN port fails or is disabled when the portmonitoring parameter is set to ON. The options are:

1...254	Specifies a value to decrement the priority of the virtual router.
proportional	Specifies that the virtual router reduces the priority in proportion to the percentage of available ports.

delay — Specifies the number of seconds that a higher priority switch must wait before preempting a lower priority switch. This parameter is only valid when the preempt parameter is set to ON. After the switch assumes the highest priority, it waits the delay time and then assumes control. A delay ensures that there is enough time for the master to update its routing tables before taking over. The range is 0 to 3600 and the default is 0 (off).

Description

This command creates a VRRP virtual router. If other VRRP virtual routers have been created on the LAN with the same VRID, the combined group forms a single virtual router.

Note
You must create the virtual router on at least two switches for VRRP to operate correctly.

Note
All switches involved in a virtual router must be configured with the same values for the VRID, IP ADDRESSS, ADINTERVAL, PREEMPT, AUTHENTICATION and PASSWORD values in order to operate properly.

Example

This example creates a virtual router with a VRID of 7, an IP address of 12.37.8.2 over VLAN2-0, with port monitoring enabled and a stepvalue of 45:

```
create vrrp=7 over=vlan2-0 ip=12.37.8.2 portmonitoring=on
stepvalue=45
```

AlliedWare Plus Command

Syntax

To assign an ID to a new virtual router:

```
router vrrp vrid
```

To assign the interface and a secondary IP address:

```
virtual-ip ipaddress interface
```

To assign the interval in seconds between advertisement packets:

```
advertisement-interval value
```

To set authentication to plaintext:

```
password password
```

To set authentication to none:

```
no authentication
```

To enable or disable port monitoring:

```
port-monitor true|false
```

To specify whether or not ports should reset when a virtual router transitions from backup to master status:

```
port-reset true|false
```

To specify whether a higher priority switch preempts a lower priority switch acting as the master:

```
preempt-mode true|false
```

To set the priority:

```
priority value
```

To set the step value:

```
step-value value|proportional
```

To set the delay value:

```
delay value
```

Modes

For the ROUTER VRRP command:

Configure mode

For all the other commands:

Router mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example creates a virtual router with the VRID 12 and the IP address 149.42.11.12 for the VLAN5-0 interface. The virtual router uses plaintext authentication with the password “wen52an” and port monitoring:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 12
awplus(config-router)# virtual-ip 149.42.11.12 vlan5-0
awplus(config-router)# password wen52an
awplus(config-router)# port-monitor true
```

This example creates a virtual router with the VRID 7 and the IP address 182.112.45.22 for the VLAN12-4 interface. The priority and step values are set to 200 and the delay value to 500:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 7
awplus(config-router)# virtual-ip 182.112.45.22 vlan12-4
awplus(config-router)# priority 200
awplus(config-router)# step-value 200
awplus(config-router)# delay 500
```

DELETE VRRP IPADDRESS

AlliedWare Plus
Command
Available

Syntax

```
delete vrrp=vrid ipaddress=ipaddress
```

Parameters

vrrp
Specifies the ID of the virtual router, a number between 1 and 255.

ipaddress
Specifies a secondary IP address to be deleted from the group of IP addresses backed up by the specified virtual router.

Description

This command deletes a secondary IP address from the group of IP addresses backed up by the specified virtual router.

Example

This example deletes the IP address 205.42.19.162 from the group of IP addresses that are backed up by the virtual router whose VRID is 34:

```
delete vrrp=34 ipaddress=205.42.19.162
```

AlliedWare Plus Command

Syntax

```
router vrrp vrid
no interface ipaddress
```

Modes

For the ROUTER VRRP command:

Configure mode

For the NO INTERFACE command:

Router mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This example removes the IP address 172.112.45.78 from a virtual router with the VRID 12:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 12
awplus(config-router)# no interface 172.112.45.78
```

DELETE VRRP MONITOREDINTERFACE

Syntax

```
delete vrrp=vrid monitoredinterface=interface
```

Parameters

vrrp	Specifies the ID of the virtual router, a number between 1 and 255.
monitoredinterface	Specifies the monitored interface to be deleted. An interface name consists of “VLAN” followed by the name or ID (VID) of the VLAN and the interface number (e.g., vlan-Sales-0 or vlan4-0).

Description

This command deletes a monitored interface.

Example

This example deletes the VLAN1-0 interface from the group of interfaces monitored by the virtual router with a VRID of 8:

```
add vrrp=8 monitoredinterface=VLAN1-0
```

DESTROY VRRP

AlliedWare Plus Command Available

Syntax

```
destroy vrrp=[vrid|all]
```

Parameters

vrrp	Specifies the ID of the virtual router. The options are:	
	vrid	Specifies the ID of a single virtual router, a number between 1 and 255.
	all	Specifies that the switch be removed from all the virtual routers in which it participates.

Note
To destroy a virtual router completely on the LAN, you must destroy it on all the switches participating in it.

Description

This command removes the switch from the group that forms the specified VRRP virtual router.

Example

This command stops the switch from participating in virtual router 32:

```
destroy vrrp=32
```

AlliedWare Plus Command

Syntax

```
router vrrp vrid
no virtual-ip
```

Modes

For the ROUTER VRRP command:

Configure mode

For the NO VIRTUAL-IP command:

Router mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

This example deletes a virtual router with the VRID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 5
awplus(config-router)# no virtual-ip
```

DISABLE VRRP

AlliedWare Plus
Command
Available

Syntax

```
disable vrrp[=vrid|all]
```

Parameters

vrrp — Specifies the ID of the virtual router. The options are:

- vrid — Specifies the ID of a single virtual router, a number between 1 and 255.
- all — Specifies that the switch be removed from all the virtual routers in which it participates.

Description

This command disables VRRP on the switch or disables a switch's participation in the specified virtual router. VRRP is disabled on the switch by default, and virtual routers are enabled by default when you create them. You must enable both VRRP and the virtual router for the virtual router to operate.

Example

This command disables VRRP on the switch:

```
disable vrrp
```

This command stops the switch from participating in virtual router 32:

```
disable vrrp=32
```

AlliedWare Plus Command

Syntax

```
router vrrp vrid
disable
```

Modes

For the ROUTER VRRP command:

Configure mode

For the DISABLE command:

Router mode

Description

These AlliedWare Plus commands are used to disable individual virtual routers. To disable VRRP on the switch, use the standard DISABLE VRRP command.

Example

This example disables a virtual router with the VRID 2:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 2
awplus(config-router)# disable
```

ENABLE VRRP

AlliedWare Plus
Command
Available

Syntax

```
enable vrrp[=vrid|all]
```

Parameters

vrrp Specifies the ID of the virtual router. The options are:

vrid Specifies the ID of a single virtual router, a number between 1 and 255.

all Specifies that all the virtual routers in which the switch participates be enabled.

Description

This command enables VRRP on the switch, or enables the switch’s participation in a specific virtual router. VRRP is disabled on the switch by default, and virtual routers are enabled by default when you create them. You must enable both VRRP and the virtual router for the virtual router to operate.

Example

This example enables the switch to participate in virtual router 42:

```
enable vrrp=42
```

AlliedWare Plus Command

Syntax

```
router vrrp vrid
enable
```

Modes

For the ROUTER VRRP command:

Configure mode

For the DISABLE command:

Router mode

Description

These AlliedWare Plus commands are used to enable individual virtual routers. To enable VRRP on the switch, use the standard ENABLE VRRP command.

Example

This example enables a virtual router with the VRID 8:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 8
awplus(config-router)# enable
```

SET VRRP

AlliedWare Plus Command Available

Syntax

```
set vrrp=vrid [adinterval=1...255]
[authentication=none|plaintext] [password=password]
[portnomitoring=on|off] [portreset=on|off] [preempt=on|off]
[priority=1..254] [stepvalue=1..254|proportional]
[delay=0..3600]
```

Parameters

vrrp — Specifies the ID of the virtual router, a number between 1 and 255.

adinterval — Specifies the interval in seconds between advertisement packets. The range is 1 to 255 seconds and the default is 1 second. You must configure all switches in the same virtual router with the same adinterval.

authentication — Specifies whether there is password protection. Options are:

- none — Specifies no password protection. This is the default setting.
- plaintext — Specifies that a password is required, which you set with the password parameter.

password — Specifies the password used to authenticate VRRP packets. The password can be up to 16 alphanumeric characters. The password is case sensitive and can include the hyphen and underscore.

Passwords are sent in plaintext. The AT-S63 Management Software does not support encrypted passwords.

You must configure all switches in the same virtual router with the same password.

portmonitoring — Specifies whether the VRRP should monitor the ports of the VLAN and alter the priority value if ports fail or are disabled. The options are:

- on — Specifies that port monitoring should be on.

off Specifies that port monitoring should be off.This is the default.

portreset

Specifies that ports of a VLAN that has a virtual router be reset when a virtual router transitions from backup to master status. The options are:

on Specifies that the VLAN ports be reset.

off Specifies that the VLAN ports are not reset.

preempt

Specifies whether a higher priority switch preempts a lower priority switch acting as the master. The preferred master (with a priority of 255) always assumes the master role when it is available, regardless of how this parameter is set. The options are:

on Specifies that preempting should occur. This is the default.

off Specifies that preempt mode not be used.

You must configure all switches in the same virtual router with the same preempt setting.

priority

Specifies the switch's priority for becoming the master for the virtual router. The higher the value, the greater the priority. The value of 255 is reserved for the switch that is the preferred master (the switch owning the virtual router's IP address). The value of 255 is always assigned to the preferred master, regardless of how this parameter is set. The range is 1 to 254 and the default is 100.

stepvalue

Specifies the value by which the priority of the virtual router should be decremented each time a VLAN port fails or is disabled when the portmonitoring parameter is set to ON. The options are:

1...254 Specifies a value to decrement the priority of the virtual router.

proportional Specifies that the virtual router reduces the priority in proportion to the percentage of available ports.

delay	Specifies the number of seconds that a higher priority switch must wait before preempting a lower priority switch. This parameter is only valid when the preempt parameter is set to ON. After the switch assumes the highest priority, it waits the delay time and then assumes control. A delay ensures that there is enough time for the master to update its routing tables before taking over. The range is 0 to 3600 and the default is 0 (off).

Description

This command modifies the settings of a specified virtual router.

Examples

This example activates the port monitoring feature on a virtual router with a VRID of 7, and sets the step value to 15:

```
set vrrp=7 portmonitoring=on stepvalue=15
```

AlliedWare Plus Command

Syntax

To specify the ID of the virtual router you want to modify:

```
router vrrp vrid
```

To change the interval in seconds between advertisement packets:

```
advertisement-interval value
```

To change authentication to plaintext:

```
password password
```

To change authentication to none:

```
no authentication
```

To enable or disable port monitoring:

```
port-monitor true|false
```

To specify whether or not ports should reset when a virtual router transitions from backup to master status:

```
port-reset true|false
```

To specify whether a higher priority switch preempts a lower priority switch acting as the master:

```
preempt-mode true|false
```

To change the priority:

```
priority value
```

To change the step value:

```
step-value value|proportional
```

To change the delay value:

```
delay value
```

Mode

For the ROUTER VRRP command:

Configure mode

For all the other commands:

Router mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example modifies the virtual router with the VRID 12. The step value is changed to 100 and the delay value to 200:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 12
awplus(config-router)# step-value 100
awplus(config-router)# delay 200
```

This example modifies the virtual router with the VRID 7. Port monitoring and port resets are disabled:

```
awplus> enable
awplus# configure terminal
awplus(config)# router vrrp 7
awplus(config-router)# port-monitor false
awplus(config-router)# port-reset false
```

SHOW VRRP

AlliedWare Plus Command Available

Syntax

```
show vrrp[=vrid|all]
```

Parameters

vrrp Specifies the ID of the virtual router. The options are:

vrid	Specifies an ID of a virtual router you want to display. The number can be from 1 and 255.
all	Displays all of the virtual routers.

Description

This command is used to display information about the virtual routers. You can display all of them or specific virtual routers.

Figure 89 is an example of the information displayed by this command.

```
Virtual Router Identifier ................1

Configuration
  VR MAC Address ..................... 00-00-5R-00-01-01
  Interface ......................... VLAN
  Priority .......................... 34
  State ............................. Backup
  Authentication .................... Plaintext
  Password .......................... Set
  IP Address(es) .................... 34.12.163.156
  Advertisement Interval ............ 1
  Preempt Mode ...................... ON
  Preempt Delay (seconds) ........... 60
  Original Priority ................. 34
  Port Monitoring ................... ON
  Step Value ........................ 40
  Port Reset ........................ ON
Monitored Interfaces
  Interface ......................... VLAN
   New Priority ..................... 40
Counters
  Good Advertisements Received ....... 0
  Bad Advertisements Received ........ 0
  Master Periods ..................... 1
  Advertisements Sent ................ 0
```

Figure 89. SHOW VRRP Command

The information in the display is described in Table 26.

Table 26. SHOW VRRP Command Information

Section	Parameter	Description
	Virtual Router Identifier	Virtual router identifier.
Configuration	VR MAC Address	Virtual router's MAC address, derived from the virtual router identifier.
	Interface	LAN interface that the virtual router is operating on.
	Priority	Priority of the switch for assuming the master role for the virtual router.
	State	Current status of the switch in the virtual router which may be master, backup, or initial. Initial indicates that either the virtual router or VRRP is disabled.
	Authentication	If the virtual router uses no authentication or plaintext or HMAC authentication.
	Password	Whether or not the password is set.
	IP Address(es)	Shows the IP addresses associated with the virtual router.
	Advertisement Interval	Period in seconds between advertisement packets.
	Preempt Mode	Whether preempt mode is on. When on, the switch determines whether a higher priority switch assumes the master role over one with lower priority.
	Preempt Delay (seconds)	Period in seconds that the switch delays before assuming the master role after it has determined that its priority is greater than all other switches. Valid only when preempt mode is on.
	Original Priority	The original priority of the port before being affected by either the port monitoring or monitored interface feature.
	Port Monitoring	Whether the port monitoring feature is on. This parameter is displayed only when the virtual router operates over a VLAN interface.

Table 26. SHOW VRRP Command Information (Continued)

Section	Parameter	Description
	Step Value	If a number is displayed, this is the value by which the priority of the virtual router is reduced by each VLAN port that fails or is disabled. If “Proportional” is shown, the priority is reduced in proportion to the percentage of VLAN ports that are out of service.
	Port Reset	Whether port reset is on. When on, the ports of a VLAN that has a virtual router are reset when a virtual router transitions from backup to master status.
Monitored Interfaces	Interface	The name of an interface being monitored by VRRP for this virtual router.
	New Priority	The new priority that the switch uses when this interface becomes inoperative.
Counters	Good Advertisements Received	Number of acceptable advertisement packets received by the switch for this virtual router.
	Bad Advertisements Received	Number of unacceptable advertisement packets received by the switch for this virtual router.
	Master Periods	Number of periods when the switch has been the master switch.
	Advertisements Sent	Number of advertisement packets sent by the switch.

Example

This example displays the information about virtual router 16:

```
show vrrp=16
```

AlliedWare Plus Command

Syntax

```
show vrrp
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command displays all of the virtual routers. Unlike the standard command, you cannot specify individual virtual routers.

Example

```
awplus# show vrrp
```

Section VIII

Port Security

This section contains the following chapters:

- Chapter 41, “MAC Address-based Port Security Commands” on page 793
- Chapter 42, “802.1x Port-based Network Access Control Commands” on page 805

Chapter 41

MAC Address-based Port Security Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following command:

SET SWITCH PORT INTRUSIONACTION

AlliedWare Plus Command Available

Syntax

set switch port=*port* intrusionaction=discard|trap|disable

Parameters

port — Specifies the port where you want to change the intrusion action. You can specify more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

intrusionaction — Specifies the action the port takes when it receives an invalid frame. The options are:

- discard — The switch discards invalid frames on the port. This is the default.
- trap — The switch discards invalid frames on the port and sends an SNMP trap.
- disable — The switch discards invalid frames on the port, sends an SNMP trap, and disables the port.

Description

This command, which applies only to ports operating in the Limited security mode, defines the response of the switch when a port receives an invalid frame.

Example

The following command sets the intrusion action to trap on ports 12 and 21:

```
set switch port=12,21 intrusionaction=trap
```

AlliedWare Plus Command

Syntax

To set a port to discard invalid packets:

```
switchport port-security violation protect
```

To set a port to discard invalid packets and to send SNMP traps:

```
switchport port-security violation restrict
```

To set a port to discard invalid packets, to send SNMP traps, and to disable the port:

```
switchport port-security violation shutdown
```

Mode

Port Interface mode

Description

These AlliedWare Plus commands are identical to the standard command.

Example

This example sets the intrusion action on ports 22 to 24 discard the invalid packets and send SNMP traps:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22-24
awplus(config-if)# switchport port-security violation
restrict
```

SET SWITCH PORT SECURITYMODE

AlliedWare Plus
Command
Available

Syntax

```
set switch port=port
[securitymode=automatic|limited|secured|locked]
[intrusionaction=discard|trap|disable]
[learn=value] [participate=yes|no|on|off|true|false]
```

Parameters

port — Specifies the port where you want to set security. You can specify more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

securitymode — Specifies the port’s security mode. Options are:

- automatic — Disables security on the port. This is the default setting.
- limited — Sets the port to the Limited security mode. The port learns a limited number of dynamic MAC addresses, set with the LEARN parameter.
- secured — Sets the port to the Secured security mode. The port accepts frames based only on static MAC addresses. You must enter the static MAC addresses of the nodes with frames the port is to accept after you have activated this security mode on a port. To add static MAC addresses, use the command “ADD SWITCH FDB|FILTER” on page 192.
- locked — Sets the switch to the Locked security mode. The port stops learning new dynamic MAC addresses. The port forwards frames based on static MAC addresses and on those dynamic addresses it has already learned.

Note
The online help for this command includes a “pacontrol” option for this parameter. The option is nonfunctional.

intrusionaction Specifies the action taken by the port in the event port security is violated. This parameter applies only to the Limited security mode. Intrusion actions are:

discard Discards invalid frames. This is the default setting.

trap Discards invalid frames and sends a management trap.

disable Discards invalid frames, sends a management trap, and disables the port.

The intrusion action of a port operating in the Secured or Locked security level is to discard invalid frames.

learn Specifies the maximum number of dynamic MAC addresses a port on the switch can learn. This parameter applies only to ports set to the Limited security mode. The range is 1 to 255 addresses. The default is 255.

participate Enables or disables the intrusion action on the port. This option only applies to the Limited security mode and only when a port’s intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard. The options are:

yes, on, true Enables the trap or disable intrusion action. These options are equivalent.

no, off, false Disables the trap or disable intrusion action. The port still discards invalid ingress frames. This is the default. These options are equivalent.

Description

This command sets and configures a port’s security mode. Only one mode can be active on a port at a time.

To view a port’s current security mode, use the command “SHOW SWITCH PORT SECURITYMODE” on page 802.

The management software displays a confirmation prompt whenever you perform this command. Responding with **Y** for yes completes your command, while **N** for no cancels the command.

Examples

The following command sets the security level for port 8 to the Limited mode and specifies a limit of 5 dynamic MAC addresses. Because no intrusion action is specified, the discard action is assigned by default:

```
set switch port=8 securitymode=limited learn=5
```

The following command sets the security level for ports 9 and 12 to the Limited mode and specifies a limit of 15 dynamic MAC addresses per port. The disable intrusion action is specified:

```
set switch port=9,12 securitymode=limited learn=15
intrusionaction=disable participate=yes
```

In the above example, the Participate option is required to activate the disable intrusion action. Without it, the port would discard invalid ingress frames but would not send an SNMP trap and disable the port.

The following command changes the maximum number of learned MAC addresses to 150 on ports 15 and 16. The command assumes that the ports have already be set to the Limited security mode:

```
set switch port=15-16 learn=150
```

The following command sets the security level to Locked for ports 2, 6, and 18:

```
set switch port=2,6,18 securitymode=locked
```

The Limit and Participate options are not included with the above command because they do not apply to the Locked mode or the Secured mode.

The following command sets the security level to Secured for ports 12 to 24:

```
set switch port=12-24 securitymode=secured
```

The following command returns ports 8 to 11 to the automatic security level, which disables port security:

```
set switch port=8-11 securitymode=automatic
```

AlliedWare Plus Command

Syntax

To set a port to the limited security mode and to specify the maximum number of addresses a port can learn:

```
switchport port-security maximum value
```

Mode

Port Interface mode

Description

This command lets you set ports to the limited security mode. You cannot use the AlliedWare Plus commands to set ports to the Secured or Locked security mode.

Example

This example sets port 2 to the limited security mode and configures the maximum number of MAC addresses the port can learn to 15:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2
awplus(config-if)# switchport port-security maximum 15
```

SHOW SWITCH PORT INTRUSION

AlliedWare Plus
Command
Available

Syntax

```
show switch port=port intrusion
```

Parameter

port	Specifies the port where you want to view the number of intrusions that have occurred. You can specify more than one port at a time.

Description

This command displays the number of times a port has detected an intrusion violation. An intrusion violation varies depending on the security mode:

- ❒ Limited Security Level - An intrusion is an ingress frame with a source MAC address not already learned by a port after the port had reached its maximum number of dynamic MAC addresses, or that was not assigned to the port as a static address.
- ❒ Secured Security Level - An intrusion is an ingress frame with a source MAC address that was not entered as a static address on the port.
- ❒ Locked - An intrusion is an ingress frame with a source MAC address that the port has not already learned or that was not assigned as a static address.

Example

The following command displays the number of intrusion violations detected on ports 12 and 21:

```
show switch port=12,21 intrusion
```

AlliedWare Plus Command

Syntax

```
show port-security intrusion interface port
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show port-security intrusion interface 15
```

SHOW SWITCH PORT SECURITYMODE

AlliedWare Plus Command Available

Syntax

```
show switch port=port securitymode
```

Parameters

port	Specifies the port whose security mode settings you want to view. You can display more than one port at a time. For instructions on how to enter port numbers, refer to “Port Numbers in Commands” on page 48.

Description

This command displays the security mode settings for the ports on the switch. An example of the information displayed by this command is shown in Figure 90.

```
Port   Security Mode      Intrusion Action   Participating    MAC Limit
--------------------------------------------------------------------------
1      Secured            ----               ----             ----
2      Limited            Trap               Yes              20
3      Limited            Trap               Yes              20
4      Limited            Trap               Yes              20
5      Automatic          ----               ----             ----
6      Automatic          ----               ----             ----
```

Figure 90. SHOW SWITCH PORT SECURITYMODE Command

The columns in the display are defined here:

- Port - Port number.
- Security Mode - The current security mode of the port. Possible settings are Automatic (no security), Limited, Secured, and Locked. For definitions of the security levels, refer to “SET SWITCH PORT SECURITYMODE” on page 796.
- Intrusion Action - The action taken by a port operating with the Limited security level when it detects an intrusion violation.
- Participating - The status of intrusion action on the port. This option only applies to the Limited security mode and only when a port’s intrusion action is set to trap or disable. This option does not apply when intrusion action is set to discard.
- MAC Limit - The maximum number of dynamic MAC addresses the port can learn. This parameter applies only to the Limited security mode.

Example

The following command displays the security mode settings for ports 1 to 5:

```
show switch port=1-5 securitymode
```

AlliedWare Plus Command

Syntax

```
show port-security interface port
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show port-security interface 5-8
```

Chapter 42

802.1x Port-based Network Access Control Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

- "DISABLE PORTACCESS|PORTAUTH" on page 806
- "DISABLE RADIUSACCOUNTING" on page 807
- "ENABLE PORTACCESS|PORTAUTH" on page 808
- "ENABLE RADIUSACCOUNTING" on page 809
- "SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR" on page 810
- "SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT" on page 821
- "SET RADIUSACCOUNTING" on page 824
- "SHOW PORTACCESS|PORTAUTH" on page 826
- "SHOW PORTACCESS|PORTAUTH PORT" on page 828
- "SHOW RADIUSACCOUNTING" on page 831

Note
Remember to save your changes with the SAVE CONFIGURATION command.

DISABLE PORTACCESS|PORTAUTH

AlliedWare Plus Command Available

Syntax

```
disable portaccess|portauth
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

None.

Description

This command disables 802.1x Port-based Network Access Control on the switch. This is the default setting.

Example

The following command disables 802.1x Port-based Network Access Control on the switch:

```
disable portaccess
```

AlliedWare Plus Command

Syntax

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

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no dot1x system-auth-ctrl
```

DISABLE RADIUSACCOUNTING

Syntax

```
disable radiusaccounting
```

Parameters

None

Description

This command disables RADIUS accounting on the switch.

Example

The following command disables RADIUS accounting:

```
disable radiusaccounting
```

Equivalent Command

```
set radiusaccounting status=disabled
```

For information, see “SET RADIUSACCOUNTING” on page 824.

ENABLE PORTACCESS|PORTAUTH

AlliedWare Plus Command Available

Syntax

```
enable portaccess|portauth
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

None.

Description

This command activates 802.1x Port-based Network Access Control on the switch. The default setting for this feature is disabled.

Note
You should activate and configure the RADIUS client software on the switch before activating port-based access control. Refer to "SET AUTHENTICATION" on page 893.

Example

The following command activates 802.1x Port-based Network Access Control on the switch:

```
enable portaccess
```

AlliedWare Plus Command

Syntax

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

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# dot1x system-auth-ctrl
```

ENABLE RADIUSACCOUNTING

Syntax

```
enable radiusaccounting
```

Parameters

None

Description

This command activates RADIUS accounting on the switch.

Example

The following command activates RADIUS accounting:

```
enable radiusaccounting
```

Equivalent Command

```
set radiusaccounting status=enabled
```

For information, see “SET RADIUSACCOUNTING” on page 824.

SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR

AlliedWare Plus
Command
Available

Syntax

```
set portaccess|portauth=8021x|macbased port=port
type|role=authenticator|none [mode=single|multi]
[control=auto|authorised|forceauthenticate|
unauthorised|forceunauthenticate]
[quietperiod=value] [txperiod=value]
[reauthenabled=enabled|disabled] [reauthperiod=value]
[supptimeout=value] [servertimeout|servtimeout=value]
[maxreq=value] [ctrldirboth=ingress|both]
[piggyback=enabled|disabled] [guestvlan=vlan-name|vid|none]
[vlanassignment=enabled|disabled] [securevlan=on|off]
```

Parameters

portaccess **or** portauth
: Specifies the authentication method. The two choices are:

8021x
: Specifies 802.1x username and password authentication. With this authentication method a supplicant must provide, either manually or automatically, a username and password. This authentication method requires 802.1x client software on the supplicant nodes.

macbased
: Specifies MAC address-based authentication. The authenticator port extracts the source MAC address from the initial frames received from a supplicant and automatically sends the address as both the username and password of the supplicant to the authentication server. This authentication method does not require 802.1x client software on the supplicant nodes.

port
: Specifies the port to set to the Authenticator role or whose Authenticator settings you want to adjust. You can specify more than one port at a time.

type ***or*** role — Specifies the role of the port. The parameters are equivalent. The options are:

- authenticator — Specifies the authenticator role.
- none — Disables port-based access control on the port.

mode — Controls the operating mode of an authenticator port. The options are:

- single — Configures the port to accept only one authentication. This authenticator mode should be used together with the piggy-back mode. When an authenticator port is set to the single mode and the piggy-back mode is disabled, only the one client who is authenticated can use the port. Packets from or to other clients on the port are discarded. If piggy-back mode is enabled, other clients can piggy-back onto another client's authentication and so be able to use the port. This is the default setting.
- multi — Configures the port to accept up to 320 authentications. Every client using an authenticator port in this mode must have a username and password combination and log on separately.

control — Specifies the authenticator state. The options are:

- auto — Sets the port state to 802.1X port-based authentication. The port begins in the unauthorized state, allowing only EAPOL frames to be sent and received through the port. The authentication process begins when the link state of the port changes. The switch requests the identity of the client and begins relaying authentication messages between the client

		and the authentication server. Each client that attempts to access the network is uniquely identified by the switch by using the client's MAC address. This is the default setting.
	authorised ***or*** forceauthenticate	Disables 802.1X port-based authentication and causes the port to transition to the authorized state without any authentication exchange required. The port transmits and receives normal traffic without 802.1X-based authentication of the client. The parameters are equivalent.
	unauthorised ***or*** forceunauthenticate	Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch blocks all authentication on the port. The parameters are equivalent.
quietperiod	Sets the number of seconds that the switch remains in the quiet state following a failed authentication exchange with the client. The default value is 60 seconds. The range is 0 to 65,535 seconds.	
txperiod	Sets the number of seconds that the switch waits for a response to an EAP-request/identity frame from the client before retransmitting the request. The default value is 30 seconds. The range is 1 to 65,535 seconds.	
reauthenabled	Controls whether the client must periodically reauthenticate. The options are:	
	enabled	Specifies that the client must periodically reauthenticate. This is the default setting. The time period between reauthentications is set with the reauthperiod parameter.
	disabled	Specifies that reauthentication by the client is not required after the initial authentication. Reauthentication is only required if there is a change to the status of the link between the supplicant and

the switch or the switch is reset or power cycled.

reauthperiod Enables periodic reauthentication of the client, which is disabled by default. The default value is 3600 seconds. The range is 1 to 65,535 seconds.

supptimeout Sets the switch-to-client retransmission time for the EAP-request frame. The default value for this parameter is 30 seconds. The range is 1 to 600 seconds.

servertimeout ***or*** servtimeout Sets the timer used by the switch to determine authentication server timeout conditions. The default value is 30 seconds. The range is 1 to 600 seconds. The parameters are equivalent.

maxreq Specifies the maximum number of times that the switch retransmits an EAP Request packet to the client before it times out the authentication session. The range is 1 to 10 retransmissions and the default is 2.

ctrldirboth Specifies how the port is to handle ingress and egress broadcast and multicast packets when in the unauthorized state.

When a port is set to the authenticator role, it remains in the unauthorized state until a client is authenticated by the authentication server. In the unauthorized state, a port accepts only EAP packets from the client. All other ingress packets a port might receive from the supplicant, including multicast and broadcast traffic, are discarded until the supplicant has been authenticated.

You can use this selection to control how an authenticator port handles egress broadcast and multicast traffic when in the unauthorized state. You can instruct the port to forward this traffic to the client, even though the client has not logged on, or you can have the port discard the traffic.

The options are:

ingress An authenticator port, when in the unauthorized state, discards all ingress broadcast and multicast packets from the client while forwarding all egress broadcast and multicast traffic to the same client. This is the default setting.

both An authenticator port, when in the unauthorized state, does not forward ingress or egress broadcast and multicast packets from or to the client until the client has logged on.

This parameter is only available when the authenticator's operating mode is set to single. When set to multiple, an authenticator port does not forward ingress or egress broadcast or multicast packets until at least one client has logged on.

piggyback Controls who can use the switch port in cases where there are multiple clients using the port, for example the port is connected to an Ethernet hub. This parameter is applicable when the authenticator's operating mode is set to single. The options are:

enabled Allows all clients on the port to piggy-back onto the initial client's authentication, causing the port to forward all packets after one client is authenticated. This is the default setting.

disabled Specifies that the switch port forward only those packets from the client who is authenticated and discard packets from all other users.

guestvlan Specifies the name or VID of a Guest VLAN. The authenticator port is a member of a Guest VLAN when no supplicant is logged on. Clients do not log on to access a Guest VLAN.

If an authenticator port where a Guest VLAN has been defined starts to receive EAPOL packets, signalling that a supplicant is logging on, it changes to the unauthorized state and moves from the Guest VLAN to its predefined VLAN. The port remains in the unauthorized state until the log on process between the supplicant and the RADIUS server is completed.

The options are:

vlan-name Specifies the name of the Guest VLAN.

vlan-id Specifies the VID of the Guest VLAN.

none Removes a predefined Guest VLAN from an authenticator port.

A Guest VLAN is only supported when the operating mode of the port is set to Single. The specified VLAN must already exist on the switch.

vlanassignment Specifies whether to use the VLAN assignments entered in the user accounts on the RADIUS server. Options are:

enabled Specifies that the authenticator port is to use the VLAN assignments returned by the RADIUS server when a supplicant logs on. This is the default setting.

disabled Specifies that the authenticator port ignore any VLAN assignment information returned by the RADIUS server when a supplicant logs on. The authenticator port remains in its predefined VLAN assignment even when the RADIUS server returns a VLAN assignment when a supplicant logs on.

securevlan Controls the action of an authenticator port to subsequent authentications after the initial authentication where VLAN assignments have been added to the user accounts on the RADIUS server. This parameter only applies when the port is operating in the Multiple operating mode. Options are:

on Specifies that only those supplicants with the same VLAN assignment as the initial supplicant are authenticated. Supplicants with a different or no VLAN assignment are denied entry to the port. This is the default setting.

off Specifies that all supplicants, regardless of their assigned VLANs, are authenticated. However, the port remains in the VLAN specified in the initial authentication, regardless of the VLAN assignments of subsequent authentications.

Description

This command sets ports to the authenticator role and configures the authenticator role parameters. This command also removes port-based access control from a port.

Examples

The following command sets ports 4 to 6 to the authenticator role. The authentication method is set to 802.1x, meaning that the supplicants must have 802.1x client software and provide a username and password, either automatically or manually, when logging on and during reauthentications. The operating mode is set to Single and the piggy back mode to disabled. With these settings, only one supplicant can use each port. After a supplicant logs on, access by any other client to the same port is denied:

```
set portaccess=8021x port=4-6 role=authenticator mode=single
piggyback=disabled
```

The next command is identical to the previous example, except the authentication method is MAC address-based, meaning the authenticator ports use the MAC addresses of the supplicants as the usernames and passwords. With MAC address-based authentication, an authenticator port automatically extracts the MAC address from the initial frames received from a supplicant and sends it to the RADIUS server. The supplicants do not need 802.1x client software. Again, as in the previous example, since the operating mode is Single and the piggy back mode is disabled, only one supplicant can use each port.

```
set portaccess=macbased port=4-6 role=authenticator
mode=single piggyback=disabled
```

Note
The remaining examples are limited to the 802.1x authentication method, but apply equally to the MAC address-based authentication method.

The following command sets port 12 to the authenticator role and the operating mode to Single. The difference between this and the previous example is the piggy back mode is enabled. This configuration is appropriate when an authenticator port is supporting multiple clients, such as when a port is connected to an Ethernet hub, and you do not want to give each supplicant a separate username and password combination on the RADIUS server. With the piggy back mode enabled, all of the clients connected to the port can access it after one supplicant logs on:

```
set portaccess=8021x port=12 role=authenticator mode=single
piggyback=enabled
```

The following command sets port 22 to the authenticator role and the operating mode to Multiple. This configuration is also appropriate where there is more than one supplicant on a port. But an authenticator port in the Multiple mode requires that all supplicants have their own username and password combinations on the RADIUS server and that they log on before they can use the authenticator port on the switch:

```
set portaccess=8021x port=22 role=authenticator mode=multi
```

The following command assigns the Guest VLAN “Product_show” to authenticator ports 5 and 12. The ports function as untagged members of the VLAN and allow any network user access to the VLAN without logging on. However, should a port start to receive EAPOL packets, it assumes that a supplicant is initiating a log on and changes to the unauthorized state. After the log on is completed, the port moves to its predefined VLAN:

```
set portaccess=8021x port=5,12 role=authenticator
guestvlan=product_show
```

The following command configures port 15 as an authenticator port. This example assumes that the user accounts on the RADIUS server have VLAN assignments. With the VLANASSIGNMENT parameter set to enabled, the port processes the VLAN assignments it receives from the RADIUS server. Had this parameter been disabled, the port would ignore the VLAN assignments and leave the port in its predefined VLAN assignment. The VLAN assignment of the port is determined by the initial log on by a client. With the SECUREVLAN parameter set to enabled, only those subsequent supplicants having the same VLAN assignment as the initial supplicant are allowed to use the port:

```
set portaccess=8021x port=15 role=authenticator mode=multi
vlanassignment=enabled securevlan=on
```

The following command sets port 7 to the authenticator role, the quiet period on the port to 30 seconds, and the server timeout period to 200 seconds:

```
set portaccess=8021x port=7 role=authenticator
quietperiod=30 servtimeout=200
```

The following command configures authenticator port 5 to the multiple operating mode:

```
set portaccess=8021x port=5 role=authenticator mode=multi
```

The following command configures authenticator port 5 to the single operating mode and disables piggy backing:

```
set portaccess=8021x port=5 role=authenticator mode=single
piggyback=disabled
```

The following command removes port-based access control from ports 12 and 15:

```
set portaccess port=12,15 role=none
```

AlliedWare Plus Commands

Syntax for 802.1x Username and Password Authentication

To set a port to the authenticator role for 802.1x username and password authentication and to specify the authenticator state:

```
dot1x port-control auto
dot1x port-control force-authorized
dot1x port-control force-unauthorized
```

To remove a port from the authenticator role:

```
no dot1x port-control
```

To configure the authenticator port parameters:

```
dot1x port-control mode single|multi
dot1x quiet-period quietperiod
dot1x timeout tx-period txperiod
dot1x timeout re-authperiod reauthperiod
dot1x timeout supp-timeout supptimeout
dot1x timeout server-timeout servertimeout
dot1x max-req maxreq
dot1x port-control dir in
dot1x port-control dir both
```

To control reauthentication, which determines whether supplicants must periodically reauthenticate:

```
dot1x reauthentication
no dot1x reauthentication
```

To enable or disable the piggyback mode:

```
dot1x piggyback
no dot1x piggyback
```

To enable or disable the secure VLAN mode:

```
dot1x secure-vlan
no dot1x secure-vlan
```

To control whether an authenticator port’s VLAN assignment is set by the user account on the RADIUS server:

```
dot1x dynamic-vlan-creation enable
dot1x dynamic-vlan-creation disable
```

To return the parameters to their default values:

```
no dot1x port-control
no dot1x quiet-period
no dot1x timeout tx-period
no dot1x timeout re-authperiod
no dot1x timeout supp-timeout
no dot1x timeout server-timeout
no dot1x max-req
```

Syntax for 802.1x MAC Address-based Authentication

To set a port to MAC address-based authentication:

```
auth-mac enable
```

To remove MAC address-based authentication from a port:

```
auth-mac disable
```

Mode

Port Interface mode

Description

You cannot use the AlliedWare Plus commands to set the following authenticator port settings. To change the settings, use another management interface:

- ❐ Operating mode
- ❐ Guest VLAN

Examples

This example sets port 2 to the authenticator role with the authentication method of auto:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 2
awplus(config-if)# dot1x port-control auto
```

This example sets the reauthentication period to 10,000 seconds on ports 22 to 24:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 22-24
awplus(config-if)# dot1x timeout re-authperiod 10000
```

This example sets the supplicant timeout value to 80 seconds on ports 14, 17, and 21:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 14,17,21
awplus(config-if)# dot1x timeout supp-timeout 80
```

This command removes port 8 from the authenticator role:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 8
awplus(config-if)# no dot1x port-control
```

SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT

AlliedWare Plus
Command
Available

Syntax

```
set portaccess|portauth port=port type|role=supplicant|none
[authperiod=value] [heldperiod=value] [maxstart=value]
[startperiod=value] [username|name=name]
[password=password]
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

port — Specifies the port you want to set to the supplicant role or whose supplicant settings you want to adjust. You can specify more than one port at a time.

type ***or*** role — Specifies the role of the port. The parameters are equivalent. The options are:

- supplicant — Specifies the supplicant role.
- none — Disables port-based access control on the port.

authperiod — Specifies the period of time in seconds that the supplicant will wait for a reply from the authenticator after sending an EAP-Response frame. The range is 1 to 300 seconds. The default is 30 seconds.

heldperiod — Specifies the amount of time in seconds the supplicant refrains from trying to re-contact the authenticator in the event the end user provides an invalid username and/or password. After the time period has expired, the supplicant can attempt to log on again. The range is 0 to 65,535. The default value is 60.

maxstart — Specifies the maximum number of times the supplicant will send EAPOL-Start frames before assuming that there is no authenticator present. The range is 1 to 10. The default is 3.

startperiod — Specifies the time period in seconds between successive attempts by the supplicant to establish contact with an authenticator when there is no reply. The range is 1 to 60. The default is 30.

username ***or*** name
Specifies the username for the switch port. The parameters are equivalent. The port sends the name to the authentication server for verification when the port logs on to the network. The username can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The username is case-sensitive.

password
Specifies the password for the switch port. The port sends the password to the authentication server for verification when the port logs on to the network. The password can be from 1 to 16 alphanumeric characters (A to Z, a to z, 1 to 9). Do not use spaces or special characters, such as asterisks or exclamation points. The password is case-sensitive.

Description

This command sets ports to the supplicant role and configures the supplicant role parameters. This command also removes port-based access control from a port.

Examples

The following command sets ports 4 to 6 to the supplicant role:

```
set portacess port=4-6 role=supplicant
```

The following command sets port 8 to the supplicant role, the name to “switch22,” and the password to “bluebird”:

```
set portaccess port=8 role=supplicant name=switch22
password=bluebird
```

The following command removes port-based access control on ports 12 and 15:

```
set portaccess port=12,15 role=none
```

AlliedWare Plus Commands

Syntax

To set a port to the supplicant role:

```
dot1x port-control supplicant
```

To remove a port from the supplicant role:

```
no dot1x port-control
```

To configure the supplicant port parameters:

```
dot1x supplicant-params auth-period 1-300
```

```
dot1x supplicant-params held-period 0-65535
dot1x supplicant-params max-start 1-10
dot1x supplicant-params username username
dot1x supplicant-params password password
```

Mode

Port Interface mode

Description

These AlliedWare Plus commands are equivalent to the standard command. However, the STARTPERIOD parameter can not be set with the AlliedWare Plus commands.

Examples

This example sets ports 5 and 12 to the supplicant role:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 5,12
awplus(config)# dot1x port-control supplicant
```

This example sets port 21 to the supplicant role and changes the authentication period to 60 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 21
awplus(config)# dot1x port-control supplicant
awplus(config)# dot1x supplicant-params auth-period 60
```

This example removes port-based access control from ports 15 to 18:

```
awplus> enable
awplus# configure terminal
awplus(config)# interface 15-18
awplus(config)# no dot1x port-control
```

SET RADIUSACCOUNTING

Syntax

```
set radiusaccounting [status=enabled|disabled]
[serverport=value] [type=network]
[trigger=start_stop|stop_only]
[updateenable=enabled|disabled] [interval=value]
```

Parameters

status
Activates and deactivates RADIUS accounting on the switch. The options are:

enabled
Activates RADIUS accounting. This option is equivalent to "ENABLE RADIUSACCOUNTING" on page 809.

disabled
Deactivates the feature. This is the default. This option is equivalent to "DISABLE RADIUSACCOUNTING" on page 807.

serverport
Specifies the UDP port for RADIUS accounting. The default is port 1813.

type
Specifies the type of RADIUS accounting. The default is Network. This value cannot be changed.

trigger
Specifies the action that causes the switch to send accounting information to the RADIUS server. The options are:

start_stop
The switch sends accounting information whenever a client logs on or logs off the network. This is the default.

stop_only
The switch sends accounting information only when a client logs off.

updateenable
Specifies whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled. If you enable this feature, use the INTERVAL parameter to specify the intervals at which the switch is to send the accounting updates.

interval
Specifies the intervals at which the switch is to send interim accounting updates to the RADIUS server. The range is 30 to 300 seconds. The default is 60 seconds.

Description

RADIUS accounting is supported on those switch ports operating in the Authenticator role. The accounting information sent by the switch to a RADIUS server includes the date and time when clients log on and log off, as well as the number of packets sent and received by a switch port during a client session. This feature is disabled by default on the switch.

Examples

The following command activates RADIUS accounting and sets the trigger to stop only:

```
set radiusaccounting status=enabled trigger=stop_only
```

The following command enables the update feature and sets the interval period to 200 seconds:

```
set radiusaccounting updateenable=enabled interval=200
```

SHOW PORTACCESS|PORTAUTH

AlliedWare Plus
Command
Available

Syntax

```
show portaccess|portauth[=8021x|macbased] [config] [status]
```

Parameters

portaccess **or** portauth
Specifies the authenticator method of a port. Options are:

8021x
Displays information on the 802.1x authenticator ports.

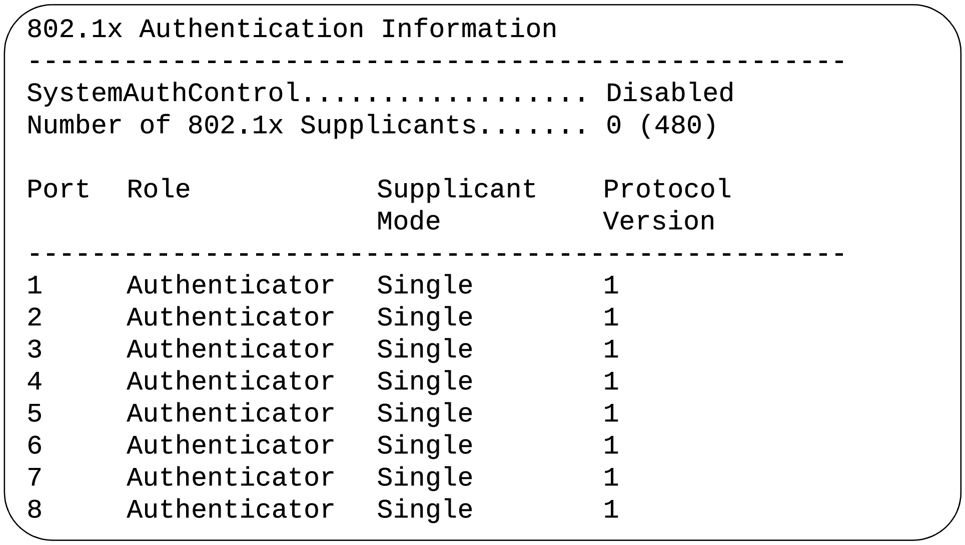
macbased
Displays information on the MAC address-based authenticator ports.

config
Displays the settings of the authenticator and supplicant ports.

status
Displays the status of the authenticator and supplicant ports.

Description

This command displays the port roles. Figure 91 is an example of the information displayed by this command.



```
802.1x Authentication Information
---------------------------------------------------
SystemAuthControl.................. Disabled
Number of 802.1x Supplicants....... 0 (480)

Port  Role           Supplicant    Protocol
                     Mode          Version
---------------------------------------------------
1     Authenticator  Single        1
2     Authenticator  Single        1
3     Authenticator  Single        1
4     Authenticator  Single        1
5     Authenticator  Single        1
6     Authenticator  Single        1
7     Authenticator  Single        1
8     Authenticator  Single        1
```

Figure 91. SHOW PORTACCESS|PORTAUTH Command

Examples

The following command displays the 802.1x authenticator ports:

```
show portaccess=8021x
```

The following command displays the MAC address-based authenticator ports:

```
show portaccess=macbased
```

AlliedWare Plus Commands

Syntax

To display the settings of the RADIUS client:

`show dot1x` statistics

To display information about the 802.1x authenticator ports:

show dot1x `interface` [*port*]

To display information about the MAC address-based authenticator ports:

show auth-mac interface *port*

Modes

User Exec mode and Privileged Exec mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Example

```
awplus# show dot1x statistics
```

```
awplus# show dot1x interface
```

```
awplus# show auth-mac interface 1-4
```

SHOW PORTACCESS|PORTAUTH PORT

AlliedWare Plus
Command
Available

Syntax

```
show portaccess|portauth[=8021x|macbased] port=port
[authenticator|supplicant]
```

Parameters

portaccess **or** portauth
Specifies the authenticator method of the port. Options are:

8021x
Displays information for an 802.1x authenticator port.

macbased
Displays information for a MAC address-based authenticator port.

port
Specifies the port whose port-based access control settings you want to view. You can specify more than one port at a time.

authenticator
Indicates that the port is an authenticator.

supplicant
Indicates that the port is a supplicant.

config
Displays the port-based access control settings for the port. Omitting this option and the STATUS option displays information on both.

status
Displays the status and role of the port. Omitting this option and the CONFIG option displays information on both.

Description

This command displays information about the authenticator ports and the supplicant ports.

Figure 92 illustrates the information displayed by this command for an authenticator port. For an explanation of the parameters, refer to “SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR” on page 810.

```
Port 1

PAE Type.................. Authenticator
Supplicant Mode........... Single
AuthControlPortControl.... Auto
quietPeriod............... 60
txPeriod.................. 30
suppTimeout............... 30
serverTimeout............. 30
maxReq.................... 2
reAuthPeriod.............. 3600
reAuthEnabled............. Enabled
vlanAssignment............ Enabled
secureVlan................ On
guestVlan................. None (VID=0)
adminControlDirection..... Both
piggyBack................. Disabled

Attached Supplicant(s)
MAC Address..................... -
   Authenticator PAE State......... Connecting
   Port Status..................... Unauthorized
   Backend Authenticator State..... Initialize
```

Figure 92. Authenticator Port Information

Figure 93 illustrates the information displayed for a supplicant port. For an explanation of the parameters, refer to “SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT” on page 821.

```
Port 5

PAE Type.................. Supplicant
heldPeriod...................... 60
authPeriod...................... 30
startPeriod..................... 30
maxStart........................ 3
Supplicant PAE State............ Connecting
```

Figure 93. Supplicant Port Information

Examples

This command displays the configuration settings and the status of all the authenticator ports and the supplicant ports:

```
show portaccess port=all
```

This command displays the configuration settings and the status for port 10:

```
show portaccess port=10
```

This command displays the configuration settings and status for port 12 which is a MAC address-based authenticator port:

```
show portaccess=macbased port=12
```

This command displays just the status information for supplicant port 17:

```
show portaccess port=17 supplicant status
```

AlliedWare Plus Command

Syntax

```
show dot1x statistics
```

```
show auth-mac interface port|all
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus SHOW DOT1X INTERFACE command displays a combination of the information from the following standard commands:

```
show portauth port=all authenticator|supplicant config
```

```
show authentication
```

For information on these commands, refer to “SHOW PORTACCESS|PORTAUTH PORT” on page 828 and “SHOW AUTHENTICATION” on page 896.

The SHOW AUTH-MAC INTERFACE command is equivalent to the MACBASED option in the standard command.

Example

```
awplus# show dot1x statistics
```

```
awplus# show auth-mac interface 1-4
```

SHOW RADIUSACCOUNTING

AlliedWare Plus
Command
Available

Syntax

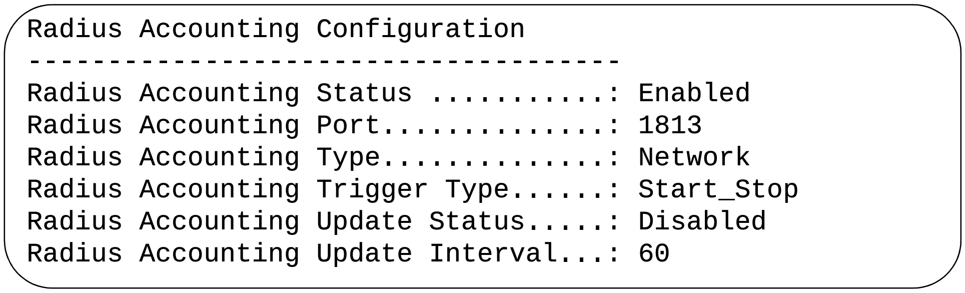
```
show radiusaccounting
```

Parameters

None.

Description

This command displays the current parameter settings for RADIUS accounting, which sends updates of supplicant activity on the switch’s authenticator ports to the RADIUS server. Figure 94 is an example of the information displayed by this command.



```
Radius Accounting Configuration
-------------------------------------
Radius Accounting Status ...........: Enabled
Radius Accounting Port..............: 1813
Radius Accounting Type..............: Network
Radius Accounting Trigger Type......: Start_Stop
Radius Accounting Update Status.....: Disabled
Radius Accounting Update Interval...: 60
```

Figure 94. SHOW RADIUSACCOUNTING Command

The information displayed by this command is described here:

- Radius Accounting Status - Specifies the status of RADIUS accounting on the switch. A status of Enabled means that the switch is sending supplicant updates to the RADIUS server: A status of Disabled means that the feature is not activated. The default is disabled.
- Radius Accounting Port - Specifies the UDP port for RADIUS accounting. The default is port 1813.
- Radius Accounting Type - Specifies the type of RADIUS accounting. The only possible setting is Network.
- Radius Accounting Trigger Type - Specifies the action that causes the switch to send accounting information to the RADIUS server. An action of Start_Stop sends accounting information whenever a client logs on or logs off the network. This is the default. An action of Stop_Only sends accounting information only when a client logs off.
- Radius Accounting Update Status - Specifies whether the switch is to send interim accounting updates to the RADIUS server. The default is disabled.

❒ Radius Accounting Update Interval - Specifies the interval at which the switch sends interim accounting updates to the RADIUS server. The default is 60 seconds.

Example

The following command displays the current parameter settings for RADIUS accounting:

```
show radiusaccounting
```

AlliedWare Plus Command

Syntax

```
show radius-acc
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Examples

```
awplus# show radius-acc
```

Section IX

Management Security

This section contains the following chapters:

Chapter 43

Web Server Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

DISABLE HTTP SERVER

AlliedWare Plus
Command
Available

Syntax

```
disable http server
```

Parameters

None.

Description

This command disables the web server on the switch. When the server is disabled, you cannot manage the switch from a web browser. To view the current status of the web server, see “SHOW HTTP SERVER” on page 844. The default setting for the web server is enabled.

Example

The following command disables the web server:

```
disable http server
```

AlliedWare Plus Command

Syntax

```
no service http
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

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

ENABLE HTTP SERVER

AlliedWare Plus Command Available

Syntax

```
enable http server
```

Parameters

None.

Description

This command activates the web server on the switch. The web server is used to manage the unit with a web browser on a remote workstation. To view the current status of the web server, see “SHOW HTTP SERVER” on page 844. The default setting for the web server is enabled.

Example

The following command activates the web server:

```
enable http server
```

AlliedWare Plus Command

Syntax

```
service http
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# service http
```

PURGE HTTP SERVER

Syntax

```
purge http server
```

Parameters

None.

Description

This command resets the HTTP server to its default values, as specified in Appendix A, “AT-S63 Default Settings” in the *AT-S63 Management Software Menus Interface User’s Guide*. To view the current web server settings, refer to “SHOW HTTP SERVER” on page 844.

Example

The following command resets the web server parameters to their default values:

```
purge http server
```

SET HTTP SERVER

Syntax

```
set http server [security=enabled|disabled] [sslkeyid=key-
id] [port=port]
```

Parameters

security — Specifies the security mode of the web server. The options are:

enabled — Specifies that the web server is to function in the secure HTTPS mode.

disabled — Specifies that the web server is to function in the non-secure HTTP mode. This is the default.

sslkeyid — Specifies a key pair ID. This parameter is required if you are configuring the web server to operate in the secure HTTPS mode.

port — Specifies the TCP port number that the web server will listen on. The defaults are port 80 for non-secure HTTP operation and port 443 for secure HTTPS operation.

Description

This command configures the web server. You can configure the server for either secure HTTPS or non-secure HTTP operation.

Before configuring the web server, please note the following:

- You cannot use this command when the web server is enabled. You must first disable the web server before making changes. To disable the server, refer to “DISABLE HTTP SERVER” on page 836.
- To configure the web server for the HTTPS secure mode, you must first create an encryption key and a certificate, and add the certificate to the certificate database. The management software will not allow you to configure the web server for the secure HTTPS mode until those steps have been completed.

Examples

The following command configures the web server for the non-secure HTTP mode. Since no port is specified, the default HTTP port 80 is used:

```
set http server security=disabled
```

The following command configures the web server for the secure HTTPS mode. It specifies the key pair ID as 5. Since no port is specified, the default HTTPS port 443 is used:

```
set http server security=enabled sslkeyid=5
```

General Configuration Steps for a Self-signed Certificate

Below are the steps you perform to configure the switch's web server for a self-signed certificate using the command line commands:

1. Set the switch's date and time. You can do this manually using "SET DATE" on page 81 or you can configure the switch to obtain the date and time from an SNTP server using "ADD SNTPSERVER PEER|IPADDRESS" on page 118.

2. Create an encryption key pair using "CREATE ENCO KEY" on page 846 (syntax 1).

3. Create the self-signed certificate using "CREATE PKI CERTIFICATE" on page 856.

4. Add the self-signed certificate to the certificate database using "ADD PKI CERTIFICATE" on page 854.

5. Disable the switch's web server using "DISABLE HTTP SERVER" on page 836.

6. Configure the web server using "SET HTTP SERVER" on page 839.

7. Activate the web server using "ENABLE HTTP SERVER" on page 837.

The following is an example of the command sequence to configuring the web server for a self-signed certificate. (The example does not include step 1, setting the system time.)

1. This command creates the encryption key pair with an ID of 4, a length of 512 bits, and the description "Switch 12 key":

   ```
   create enco key=4 type=rsa length=512 description="Switch
   12 key"
   ```

2. This command creates a self-signed certificate using the key created in step 1. The certificate is assigned the filename "Sw12cert.cer. (The ".cer" extension is not included in the command because it is added automatically by the management software.) The certificate is assigned the serial number 0 and a distinguished name of 149.11.11.11, which is the IP address of a master switch:

   ```
   create pki certificate=Sw12cert keypair=4 serialnumber=0
   subject="cn=149.11.11.11"
   ```

3. This command adds the new certificate to the certificate database. The certificate is given a description of "Switch 12 certificate":

   ```
   add pki certificate="Switch 12 certificate"
   location=Sw12cert.cer
   ```

4. This command disables the web server:

   ```
   disable http server
   ```

5. This command configures the web server by activating HTTPS and specifying the encryption key pair created in step 1:

   ```
   set http server security=enabled sslkeyid=4
   ```

6. This command enables the web server:

   ```
   enable http server
   ```

General Configuration Steps for a CA Certificate

Below are the general steps you have to perform to configure the switch's web server for CA certificates using the command line commands. The steps explain how to create an encryption key and a self-signed certificate, and how to configure the web server for the certificate:

1. Set the switch's date and time. You can do this manually using the "SET DATE" on page 81 or you can configure the switch to obtain the date and time from an SNTP server using "ADD SNTPSERVER PEER|IPADDRESS" on page 118.

2. Create an encryption key pair using "CREATE ENCO KEY" on page 846 (syntax 1).

3. Set the switch's distinguished name using "SET SYSTEM DISTINGUISHEDNAME" on page 866.

4. Create an enrollment request using "CREATE PKI ENROLLMENTREQUEST" on page 859.

5. Upload the enrollment request from the switch to a management station or TFTP server using “UPLOAD METHOD=XMODEM” on page 299 or “UPLOAD METHOD=TFTP” on page 296.

6. Submit the enrollment request to a CA.

7. After you have received the CA certificates, download them into the switch’s file system using “LOAD METHOD=XMODEM” on page 285 or “LOAD METHOD=TFTP” on page 278.

8. Add the CA certificates to the certificate database using “ADD PKI CERTIFICATE” on page 854.

9. Disable the switch’s web server using the command “DISABLE HTTP SERVER” on page 836.

10. Configure the web server using “SET HTTP SERVER” on page 839.

11. Activate the web server using “ENABLE HTTP SERVER” on page 837

Here is an example of how to configure the web server for CA certificates. It explains how to create an encryption key and enrollment request, and how to download the CA certificates to the switch. (The example does not include step 1, setting the system time, and the procedure for submitting the request to a CA, which will vary depending on the enrollment requirements of the CA.)

1. This command creates the encryption key pair with an ID of 8, a length of 512 bits, and the description “Switch 24 key”:

   ```
   create enco key=8 type=rsa length=512 description="Switch
   24 key"
   ```

2. This command sets the switch’s distinguished name to the IP address 149.44.44.44, which is the IP address of a master switch:

   ```
   set system distinguishedname="cn=149.44.44.44"
   ```

3. This command creates an enrollment request using the encryption key created in step 1. It assigns the request the filename “sw24cer.csr”. The command omits the “.csr” extension because the management software adds it automatically:

   ```
   create pki enrollmentrequest=sw24cer keypair=8
   ```

4. This command uploads the enrollment request from the switch’s file system to a TFTP server. The command assumes that the TFTP server has the IP address 149.88.88.88. (This step could also be performed using Xmodem.)

   ```
   upload method=tftp destfile=c:sw24cer.csr
   server=149.88.88.88 file=sw24cer.csr
   ```

5. These commands download the CA certificates into the switch's file system from the TFTP server. The commands assume that the IP address of the server is 149.88.88.88 and that the certificate names are "sw24cer.cer" and "ca.cer". (This step could be performed using Xmodem.)

   ```
   load method=tftp destfile=sw24cer.cer server=149.88.88.88
   file=c:sw24cer.cer
   ```

   ```
   load method=tftp destfile=ca.cer server=149.88.88.88
   file=c:ca.cer
   ```

6. These commands load the certificates into the certificate database:

   ```
   add pki certificate="Switch 24 certificate"
   location=sw24cert.cer
   ```

   ```
   add pki certificate="CA certificate" location=ca.cer
   ```

7. This command disables the web server:

   ```
   disable http server
   ```

8. This command configures the web server. It activates HTTPS and specifies the key created in step 1:

   ```
   set http server security=enabled sslkeyid=8
   ```

9. This command enables the web server:

   ```
   enable http server
   ```

SHOW HTTP SERVER

Syntax

```
show http server
```

Parameters

None.

Description

This command displays the following information about the web server on the switch:

❒ Status

❒ SSL security

❒ SSL key ID

❒ Listen port

Example

The following command displays the status of the web server:

```
show http server
```

Chapter 44

Encryption Key Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

- ❒ "CREATE ENCO KEY" on page 846
- ❒ "DESTROY ENCO KEY" on page 850
- ❒ "SET ENCO KEY" on page 851
- ❒ "SHOW ENCO" on page 852

CREATE ENCO KEY

AlliedWare Plus
Command
Available

Syntax 1

```
create enco key=key-id type=rsa length=value
[description="description"]
```

Syntax 2

```
create enco key=key-id type=rsa [description="description"]
[file=filename.key] [format=hex|ssh|ssh2]
```

Parameters

key

Specifies a key ID. The range is 0 to 65,535. The default is 0. When creating a new key this value must be unique from all other key IDs on the switch.

type

Specifies the type of key, which can only be a random RSA key.

length

Specifies the length of the key in bits. The range is 512 to 1536 bits, in increments of 256 bits (for example, 512, 768, 1024, etc). The default is 512 bits. This parameter is only used when creating a new encryption key pair.

description

Specifies a description for the encryption key. The description can be up to 40 alphanumeric characters. Spaces are allowed. The description must be enclosed in quotes. This parameter, which is optional, is used when creating a new key pair and when importing a public key from the AT-S63 file system to the key database. This parameter should not be used when exporting a public key to the file system.

file

Specifies a filename for the key. The filename must include the “.key” extension. This parameter is used when you are importing or exporting a public key from the key database. This parameter is not used when creating a new encryption key pair.

format

Specifies the format when importing or exporting a public encryption key. The options are:

hex

Specifies a hexadecimal format used to transfer a key between devices other than switches. This is the default.

ssh — Specifies a format for Secure Shell version 1 users.

ssh2 — Specifies a format for Secure Shell version 2 users.

Description

This command serves two functions. One is to create encryption keys. The other is to import and export public encryption keys from the AT-S63 file system to the key database.

Caution

Key generation is a CPU-intensive process. Because this process may affect switch behavior, Allied Telesis recommends creating keys when the switch is not connected to a network or during periods of low network activity.

Syntax 1 Description

Syntax 1 creates encryption key pairs. It creates both the public and private keys of a key pair. A new key pair is automatically stored in the key database and the file system. To view the current keys on a switch, use the “SHOW ENCO” on page 852.

The KEY parameter specifies the identification number for the key. The number must be unique from all other key pairs already on the switch. The range is 0 to 65,535. This number is used only for identification purposes and not in generating the actual encryption key pair.

The TYPE parameter specifies the type of key to be created. The only option is RSA.

The LENGTH parameter specifies the length of the key in bits. The range is 512 to 1,536 bits, in increments of 256 bits (for example, 512, 768, 1024, etc). Before selecting a key length, note the following:

- For SSL and web browser encryption, key length can be any valid value within the range.
- For SSH host and server key pairs, the two key pairs must be created separately and be of different lengths of at least one increment (256 bits) apart. The recommended length for the server key is 768 bits and the recommended length for the host key is 1024 bits.

The DESCRIPTION parameter is optional. You can use it to add a description to the key. This can help you identify the different keys on the switch. The description can be up to forty alphanumeric characters. It must be enclosed in quotes and spaces are allowed.

Syntax 1 Examples

This example creates a key with the ID of 12 and a length of 512 bits:

```
create enco key=12 type=rsa length=512
```

This example creates a key with the ID of 4, a length of 1024 bits, and a description of “Switch12a encryption key”:

```
create enco key=4 type=rsa length=1024
description="Switch12a encryption key"
```

Syntax 2 Description

Syntax 2 is used to import and export public encryption keys. You can import a public key from the AT-S63 file system to the key database or vice versa.

The only circumstance in which you are likely to use this command is if you are using an SSH client that does not download the key automatically when you start an SSH management session. In that situation, you can use this procedure to export the SSH client key from the key database into the AT-S63 file system, from where you can upload it onto the SSH management session for incorporation in your SSH client software.

You should not use this command to export an SSL public key. Typically, an SSL public key only has value when incorporated into a certificate or enrollment request.

The KEY parameter specifies the identification number for the key. The range is 0 to 65,535. To import a public key from the file system to the key database, the key ID must be unused; it cannot already be assigned to another key pair. Importing a public key to the database assumes that you have already stored the public key in the file system.

If you are exporting a public key from the key database to the file system, the KEY parameter should specify the ID of the key that you want to export. Only the public key of a key pair is exported to the file system. You cannot export a private key.

The TYPE parameter specifies the type of key to be imported or exported. The only option is RSA.

The FILE parameter specifies the filename of the encryption key. The filename must include the “.key” extension. If you are exporting a key from the key database to the file system, the filename must be unique from all other files in the file system. If you are importing a key, the filename should specify the name of the file in the file system that contains the key you want to import into the key database.

The DESCRIPTION parameter specifies a user-defined description for the key. This parameter should be used only when importing a key and not when exporting a key. The description will appear next to the key when you view the key database. Descriptions can help you identify the different keys stored in the switch.

The FORMAT parameter specifies the format of the key, which can be either Secure Shell format (SSH version 1 or 2) or hexadecimal format (HEX). The FORMAT parameter must be specified when importing or exporting keys. The default is HEX.

Syntax 2 Examples

This is an example of exporting a public key from the key database to the file system. The example assumes that the ID of the key pair with the public key to be exported is 12 and that you want to store the key as a file called "public12.key" in the file system. It specifies the format as SSH version 1 and the type as RSA:

```
create enco key=12 type=rsa file=public12.key format=ssh
```

This is an example of importing a public key from the file system to the key database. It assumes that the name of the file containing the public key is swpub24.key and that the key is to be given the ID number 6 in the key database. It gives the key the description "Switch 24 public key." The format is SSH version 2 and the type is RSA:

```
create enco key=6 type=rsa description="Switch 24 public
key" file=swpub24.key format=ssh2
```

AlliedWare Plus Command

Syntax

```
crypto key generate hostkey rsa length/key-id
```

Mode

Configure mode

Description

This command is analogous to syntax 1 of the CREATE ENCO command. It is used to create encryption key pairs. The AlliedWare Plus management interface does not have a command for importing or exporting public keys. Those functions have to be performed from another management interface.

Example

This example creates an encryption key with a length of 512 bits and the ID number 4:

```
awplus> enable
awplus# configure terminal
awplus(config)# crypto key generate hostkey rsa 512/4
```

DESTROY ENCO KEY

AlliedWare Plus
Command
Available

Syntax

```
destroy enco key=key-id
```

Parameter

key Specifies the ID number of the key pair to be deleted from the key database.

Description

This command deletes an encryption key pair from the key database. This command also deletes a key’s corresponding ”.UKF” file from the file system. After a key pair is deleted, any SSL certificate created using the public key of the key pair will be invalid and cannot be used to manage the switch. To view the keys, see “SHOW ENCO” on page 852.

You cannot delete a key pair if it is being used by SSL or SSH. You must first either disable the SSL or SSH server software on the switch or reconfigure the software by specifying another key.

Example

The following command destroys the encryption key pair with the key ID 4:

```
destroy enco key=4
```

AlliedWare Plus Command

Syntax

```
no crypto key pubkey-chain knownhosts key-id
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example deletes the encryption key pair with the key ID 5:

```
awplus> enable
awplus# configure terminal
awplus(config)# no crypto key pubkey-chain knownhosts 5
```

SET ENCO KEY

Syntax

```
set enco key=key-id description="description"
```

Parameters

key	Specifies the ID number of the key pair whose description you want to change.
description	Specifies the new description of the key. The description can contain up to 25 alphanumeric characters. Spaces are allowed. The description must be enclosed in double quotes.

Description

This command changes the description of a key pair. Descriptions can make it easier to identify the different keys on a switch.

The KEY parameter specifies the identification number of the key. The encryption key must already exist. To view the keys on a switch, see “SHOW ENCO” on page 852.

The DESCRIPTION parameter specifies the new description for the key.

Example

The following command changes the description for the key with the ID 6 to “Switch 22 key”:

```
set enco key=1 description="Switch 22 key"
```

SHOW ENCO

AlliedWare Plus
Command
Available

Syntax

```
show enco key[=key-id]
```

Parameters

key

Specifies the ID of a specific key whose information you want to display. Otherwise, all keys are displayed.

Description

This command displays information about encryption key pairs stored in the key database. This command displays the following information about each key:

- ID
- Algorithm
- Length Digest
- Description

Example

The following command displays the information for encryption key 1:

```
show enco key=1
```

AlliedWare Plus Command

Syntax

```
show crypto key hostkey
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show crypto key hostkey
```

Chapter 45

Public Key Infrastructure (PKI) Certificate Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

ADD PKI CERTIFICATE

Syntax

```
add pki certificate="name" location="filename.cer"
[trusted=yes|no|on|off|true|false] [type=ca|ee|self]
```

Parameters

certificate — Specifies a name for the certificate. This is the name for the certificate as it will appear in the certificate database list. The name can up to 40 alphanumeric characters. Spaces are allowed. If the name contains spaces, it must be enclosed in double quotes. Each certificate must be given a unique name.

location — Specifies the filename of the certificate, with the ".cer" file extension, as it is stored in the switch's file system.

trusted — Specifies whether or not the certificate is from a trusted CA. The options are:

yes, on, true	Specifies that the certificate is from a trusted CA. This is the default.
no, off, false	Specifies that the certificate is not from a trusted CA.

type — Specifies the type of certificate being added. The options are:

ca	Tags the certificate as a CA certificate.
ee	Tags the certificate as belonging to another end entity (EE). This is the default.
self	Tags the certificate as its own.

Description

This command adds a certificate to the certificate database from the AT-S63 file system. To view the certificate files in the file system, refer to "SHOW FILE" on page 272. To view the certificates already in the database, refer to "SHOW PKI CERTIFICATE" on page 868.

The CERTIFICATE parameter assigns the certificate a name. The name can be from 1 to 40 alphanumeric characters. Each certificate in the database should be given a unique name.

The LOCATION parameter specifies the filename of the certificate as stored in the switch's file system. When specifying the filename, be sure to include the file extension ".cer" .

The TRUSTED parameter specifies whether the certificate is from a trusted CA. The default is TRUE. Only self-signed root CA certificates are typically set to be automatically trusted, and only after the user has checked the certificate's fingerprint and other details using "SHOW PKI CERTIFICATE" on page 868.

The TYPE parameter specifies what type of certificate is being added. Self signed certificates should be assigned a type of SELF. If CA is specified, the switch tags this certificate as a CA certificate. If ENDENTITY or EE is specified, the switch tags the certificate to indicate that it belongs to an end entity. The default is ENDENTITY.

Note
The TRUSTED and TYPE parameters have no affect on the operation of a certificate. You can select any permitted value for either parameter, or you can omit the parameters. The parameters are included only as placeholders for information in the certificate database.

Example

The following command loads the certificate "sw12.cer" from the file system into the certificate database. The certificate is assigned the name "Switch 12 certificate":

```
add pki certificate="Switch 12 certificate"
location="sw12.cer" type=self
```

CREATE PKI CERTIFICATE

Syntax

```
create pki certificate=name keypair=key-id
serialnumber=value [format=der|pem]
subject="distinguished-name"
```

Parameters

certificate	Specifies a name for the self-signed certificate. The name can be from one to eight alphanumeric characters. Spaces are allowed; if included, the name must be enclosed in double quotes. The management software automatically adds the ".cer" extension.
keypair	Specifies the ID of the key pair that you want to use to create the certificate.
serialnumber	Specifies the serial number for the certificate. The range is 0 to 2147483647. The default is 0.
format	Specifies the type of encoding the certificate will use. The options are:

der	Specifies binary format which cannot be displayed. This is the default.
pem	Specifies an ASCII-encoded format that allows the certificate to be displayed once it is generated.

subject	Specifies the distinguished name for the certificate. The name must be enclosed in quotes.

Description

This command creates a self-signed certificate. You can use the certificate to add encryption to your web browser management sessions of the switch. A new self-signed certificate is automatically stored in the switch's file system.

Before you can create a self-signed certificate, you must create an encryption key pair. The certificate will contain the public key of the key pair. To create a key pair, refer to "CREATE PKI CERTIFICATE" on page 856.

After you have created a new self-signed certificate, you need to load it into the certificate database. The switch cannot use the certificate for encrypted web browser management systems until it is loaded into the database. For instructions, refer to "ADD PKI CERTIFICATE" on page 854.

Note
For a review of the steps to configuring the web server for a self-signed certificate, refer to "SET HTTP SERVER" on page 839.

The CERTIFICATE parameter assigns a file name to the certificate. This is the name under which the certificate will be stored as in the switch's file system. The name can be from one to eight alphanumeric characters. If the name includes a space, it must be enclosed in double quotes. The software automatically adds the extension ".cer" to the name.

The KEYPAIR parameter specifies the ID of the encryption key that you want to use to create the certificate. The public key of the pair will be incorporated into the certificate. The key pair that you select must already exist on the switch. To create a key pair, refer to "CREATE ENCO KEY" on page 846. To view the IDs of the keys already on the switch, refer to "SHOW ENCO" on page 852.

The SERIALNUMBER parameter specifies the number to be inserted into the serial number field of the certificate. A serial number is typically used to distinguish a certificate from all others issued by the same issuer, in this case the switch. Self-signed certificates are usually assigned a serial number of 0.

The FORMAT parameter specifies the type of encoding the certificate will use. PEM is ASCII-encoded and allows the certificate to be displayed once it has been generated. DER encoding is binary and so cannot be displayed. The default is DER.

The SUBJECT parameter specifies the distinguished name for the certificate. The name is inserted in the subject field of the certificate. Allied Telesis recommends using the IP address of the master switch as the distinguished name (for example, "cn=149.11.11.11"). If your network has a Domain Name System and you mapped a name to the IP address of a switch, you can specify the switch's name instead of the IP address as the distinguished name.

Examples

The following command creates a self-signed certificate. It assigns the certificate the filename “sw12.cer”. (The management software automatically adds the “.cer” extension.) The command uses the key pair with the ID 12 to create the certificate. The format is ASCII and the distinguished name is the IP address of a master switch:

```
create pki certificate=sw12 keypair=12 serialnumber=0
format=pem subject="cn=149.11.11.11"
```

The following command creates a self-signed certificate with a filename of “S45 cert”. The key pair used to create it has the ID 5. No format is specified, so the default binary format is used. The distinguished name is the IP address of another master switch:

```
create pki certificate="S45 cert" keypair=5 serialnumber=0
subject="cn=149.22.22.22"
```

CREATE PKI ENROLLMENTREQUEST

Syntax

```
create pki enrollmentrequest="name" keypair=key-id
[format=der|pem] [type=pkcs10]
```

Parameters

enrollmentrequest — Specifies a filename for the enrollment request. The filename can be from 1 to 8 alphanumeric characters. If the name contains spaces, it must be enclosed in double quotes. The management software automatically adds the “.csr” extension.

keypair — Specifies the key pair that you want to use to create the enrollment request.

format — Specifies the type of encoding the certificate request will use. The options are:

- der — Specifies binary format which cannot be displayed. This is the default.
- pem — Specifies an ASCII-encoded format that allows the certificate to be displayed once it is generated.

type — Formats the request according to PKCS #10.

Description

This command creates a certificate enrollment request. You create an enrollment request when you want a public or private CA to issue a certificate.

Before you can create an enrollment request, you must create the key pair that you want the CA to use when creating the certificate. The enrollment request will contain the public key of the key pair. To create a key pair, refer to “CREATE PKI CERTIFICATE” on page 856.

You must also set the system’s distinguished name before using this command. To set the distinguished name, refer to “SET SYSTEM DISTINGUISHEDNAME” on page 866.

> **Note**
> For a review of the steps to configuring the web server for a CA certificate, refer to “SET HTTP SERVER” on page 839.

The ENROLLMENTREQUEST parameter specifies a filename for the request. The filename can contain from 1 to 8 alphanumeric characters. If spaces are used, the name must be enclosed in quotes. The management software automatically adds the ".csr" extension. This is the filename under which the request will be stored in the file system.

The KEYPAIR parameter specifies the key that you want to use to create the enrollment request. The public key of the pair is incorporated into the request.

The FORMAT parameter specifies the type of encoding format for the request. DER specifies that the enrollment request should be written straight to the binary file. PEM specifies that the enrollment request should be encoded using the "Privacy Enhanced Mail" format. The default is DER. This parameter is only valid for manual enrollment.

The TYPE parameter specifies the type of request. The only option is PKCS10.

You do not need to use the SAVE CONFIGURATION command after you create an enrollment request. The file is permanently saved in the file system until you manually delete it.

Example

The following command creates an enrollment request. It names the enrollment request file "Switch12" and uses the key pair with the ID 4 to generate the request:

```
create pki enrollmentrequest=Switch12 keypair=4
```

DELETE PKI CERTIFICATE

Syntax

```
delete pki certificate="name"
```

Parameter

certificate	Specifies the name of the certificate you want to delete from the certificate database. The name is case sensitive. If the name contains spaces, it must be enclosed in double quotes. Wildcards are not allowed.

Description

This command deletes a certificate from the switch's certificate database. To view the certificates in the database, refer to "SHOW PKI CERTIFICATE" on page 868.

Deleting a certificate from the database does not delete it from the file system. To delete a file from the file system, refer to "DELETE FILE" on page 260.

You cannot delete a certificate from the database if you specified its corresponding encryption key as the active key in the web server configuration. The switch considers the certificate to be in use and will not allow you to delete it. You must first configure the web server with another encryption key pair for a different certificate.

Example

The following command deletes the certificate "Switch 12 certificate" from the certificate database:

```
delete pki certificate="Switch 12 certificate"
```

PURGE PKI

Syntax

```
purge pki
```

Parameters

None.

Description

This command deletes all certificates from the certificate database and resets the certificate database storage limit to the default. This command does not delete the certificates from the file system. To delete files from the file system, refer to “DELETE FILE” on page 260.

Example

The following command deletes the certificates from the database and resets the storage limit to the default:

```
purge pki
```

SET PKI CERTIFICATE

Syntax

```
set pki certificate="name"
[trusted=yes|no|on|off|true|false] [type=ca|ee|self]
```

Parameters

certificate Specifies the certificate name whose trust or type you want to change. The name is case sensitive. If the name contains spaces, it must be enclosed in quotes.

trusted Specifies whether or not the certificate is from a trusted CA. The options are:

yes, on, true Specifies that the certificate is from a trusted CA. This is the default. The options are equivalent.

no, off, false Specifies that the certificate is not from a trusted CA. The options are equivalent.

type Specifies a type for the certificate. The options are:

ca Tags the certificate as a CA certificate.

ee Tags the certificate as belonging to another end entity (EE). This is the default.

self Tags the certificate as its own.

Description

This command changes the level of trust and type for a certificate in the switch’s certificate database. To list the certificates in the database, refer to “SHOW PKI CERTIFICATE” on page 868.

The TRUSTED parameter specifies whether the certificate is from a trusted CA. The default is TRUE. Only self-signed root CA certificates are typically set to be automatically trusted, and only after the user has checked the certificate’s fingerprint and other details using “SHOW PKI CERTIFICATE” on page 868.

The TYPE parameter specifies the certificate type. If CA is specified, the switch tags this certificate as a CA certificate. If ENDENTITY or EE is specified, the switch tags the certificate to indicate that it belongs to an end entity. If SELF is specified, the switch tags the certificate as its own. The default is ENDENTITY.

Note
The TRUSTED and TYPE parameters have no affect on the operation of a certificate. You can select any permitted value for either parameter. The parameters are included only as placeholders for information in the certificate database.

Example

The following command sets the certificate named “Switch 12 certificate” to be trusted.

```
set pki certificate="Switch 12 certificate" trusted=true
```

SET PKI CERTSTORELIMIT

Syntax

```
set pki certstorelimit=value
```

Parameter

certstorelimit Specifies the maximum number of certificates the certificate database can store. The range is 12 and 256; the default is 256.

Description

This command sets the maximum number of certificates the database can store.

Example

The following command sets the certificate storage limit to 100:

```
set pki certstorelimit=100
```

SET SYSTEM DISTINGUISHEDNAME

Syntax

```
set system distinguishedname="name"
```

Parameter

distinguishedname	Specifies the distinguished name for the switch. The name must be enclosed in quotes.

Description

This command sets the distinguished name for the switch. The distinguished name is used to create a self signed certificate or enrollment request. Allied Telesis recommends using the switch's IP address or, for networks with a Domain Name System, its domain name as the distinguished name. For slave switches in an enhanced stack, which do not have an IP address, you can use the IP address or domain name of the master switch as a slave switch's distinguished name.

To set the distinguished name when creating a self signed certificate, you can use this command or you can set it directly in "CREATE PKI CERTIFICATE" on page 856, which is the command for creating a self signed certificate. It has a parameter for setting the distinguished name.

If you are creating an enrollment request, you must set the distinguished name with this command first before creating the request. The command for creating an enrollment request is "CREATE PKI ENROLLMENTREQUEST" on page 859.

Example

The following command sets the switch's distinguished name to the IP address 169.22.22.22:

```
set system distinguishedname="cn=169.22.22.22"
```

SHOW PKI

Syntax

```
show pki
```

Parameters

None.

Description

This command displays the current setting for the maximum number of certificates the switch will allow you to store in the certificate database. To change this value, refer to “SET PKI CERTSTORELIMIT” on page 865.

Example

The following command displays the current PKI settings:

```
show pki
```

SHOW PKI CERTIFICATE

Syntax

```
show pki certificate[="name"]
```

Parameter

certificate	Specifies the name of a certificate. If the name contains spaces, it must be enclosed in double quotes. This parameter is case sensitive. Wildcards are not allowed.

Description

This command lists all of the certificates in the certificates database. This command can also display information about a specific certificate in the database.

Example

The following command lists all of the certificates in the database:

```
show pki certificate
```

The following command displays information specific to the certificate “Switch 12 certificate”:

```
show pki certificate="Switch 12 certificate"
```

Chapter 46

Secure Sockets Layer (SSL) Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following command:

- “SET SSL” on page 870
- “SHOW SSL” on page 871

SET SSL

Syntax

```
set ssl [cachetimeout=value] [maxsessions=value]
```

Parameters

cachetimeout
Specifies the maximum time in seconds that a session will be retained in the cache The range is 1 to 600 seconds. The default is 300 seconds.

maxsessions
Specifies the maximum number of sessions that will be allowed in the session resumption cache. The range is 0 to 100 sessions. The default is 50 sessions.

Description

This command configures the SSL parameters.

The CACHETIMEOUT parameter determines the maximum time that a session will be retained in the cache. The cache stores information about closed connections so they can be resumed quickly. The default is 300 seconds.

The MAXSESSIONS parameter specifies the maximum number of sessions that will be allowed in the session resumption cache. The number of ENCO channels supported by the switch limits this number. The default is 50 sessions.

Example

The following command sets the session resumption cache to 180 seconds:

```
set ssl cachetimeout=180
```

SHOW SSL

Syntax

```
show ssl
```

Parameters

None.

Description

This command displays the current settings for the following SSL values:

- Version
- Available ciphers
- Maximum number of sessions
- Cache timeout

Example

The following command displays the current SSL settings:

```
show ssl
```

Chapter 47

Secure Shell (SSH) Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes

This chapter contains the following commands:

DISABLE SSH SERVER

AlliedWare Plus Command Available

Syntax

```
disable ssh server
```

Parameters

None.

Description

This command disables the Secure Shell server. When the Secure Shell server is disabled, you cannot remotely manage the unit with a Secure Shell client. The default setting for the Secure Shell server is disabled.

Example

The following command disables the Secure Shell server:

```
disable ssh server
```

AlliedWare Plus Command

Syntax

```
no service ssh
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus> enable
awplus# configure terminal
awplus(config)# no service ssh
```

ENABLE SSH SERVER

AlliedWare Plus
Command
Available

Syntax

```
enable ssh server hostkey=key-id serverkey=key-id
[expirytime=hours] [logintimeout=seconds]
```

Parameters

hostkey Specifies the ID number of the encryption key pair to function as the host key.

serverkey Specifies the ID number of the encryption key pair to function as the server key.

expirytime Specifies the length of time, in hours, after which the server key pair is regenerated. The range is 0 to 5 hours. Entering 0 never regenerates the key. The default is 0.

logintimeout Specifies the length of time the server waits before disconnecting an un-authenticated client. The range is 60 to 600 and the default is 180.

Description

This command enables the Secure Shell server and sets the server's parameters. When the Secure Shell server is enabled, you can remotely manage the device with a Secure Shell client. The default setting for the server is disabled.

The HOSTKEY parameter specifies the key ID of the host key pair. The specified key pair must already exist. To create a key pair, refer to "CREATE ENCO KEY" on page 846 (syntax 1).

The SERVERKEY parameter specifies the key of the server key pair. The specified key pair must already exist.

The EXPIRYTIME parameter specifies the time, in hours, after which the Secure Shell server key will expire and will be regenerated. If 0 is specified the key does not expire. The range is 0 to 5 and the default is 0.

The LOGINTIMEOUT parameter specifies the length of time the server waits before disconnecting an unauthenticated client. The range is 60 to 600 and the default is 180.

Note
Before you enable SSH, disable the Telnet management session. Otherwise, the security provided by SSH is not active. See "DISABLE TELNET" on page 67.

Example

The following command activates the Secure Shell server and specifies encryption key pair 0 as the host key and key pair 1 as the server key:

```
enable ssh server hostkey=0 serverkey=1
```

General Configuration Steps for SSH Operation

Configuring the SSH server involves several commands. The information in this section lists the functions and commands you need to perform to configure the SSH feature.

1. Create two encryption key pairs. One pair will function as the SSH host key and another as the SSH server key. The keys must be of different lengths of at least one increment (256 bits) apart. The recommended size for the server key is 768 bits. The recommended size for the server key is 1024 bits. To create a key pair, see to "CREATE ENCO KEY" on page 846.

2. Disable Telnet access to the switch or stack with the DISABLE TELNET command. See "DISABLE TELNET" on page 67.

   Although the AT-S63 Management Software allows the SSH and Telnet servers to be active on the device simultaneously, allowing Telnet to remain active negates the security of the SSH feature.

3. Configure and activate SSH on the device using "ENABLE SSH SERVER" on page 875.

4. Install SSH client software on your PC.

   Follow the directions provided with the client software. You can download SSH client software from the Internet. Two popular SSH clients are PuTTY and CYGWIN.

5. Log on to the SSH server from the SSH client.

   Acceptable users are those with a Manager or Operator login as well as users configured with the RADIUS and TACACS+ protocols.

Example

The following is an example of the command sequence to configuring the SSH software on the server:

1. The first step is to create the two encryption key pairs. Each key must be created separately and the key lengths must be at least one increment (256 bits) apart. The following two commands create the host and server keys using the recommended key lengths:

   ```
   create enco key=1 type=rsa length=1024 description="host
   key"
   ```

   ```
   create enco key=2 type=rsa length=768 description="server
   key"
   ```

2. The following command disables Telnet:

   ```
   disable telnet
   ```

3. The last command activates the SSH software and sets the host key as encryption key pair 1 and the server key as key pair 2:

   ```
   enable ssh server hostkey=1 serverkey=2
   ```

AlliedWare Plus Command

Syntax

service ssh *hostkey serverkey*

Mode

Configure mode

Description

You cannot set the expiry time or the login timeout value from the AlliedWare Plus commands. To set these parameters, use the standard command or another management interface.

Example

This example specifies encryption key 1 and encryption key 2 as the host key and the server key, respectively:

```
awplus> enable
awplus# configure terminal
awplus(config)# service ssh 1 2
```

SET SSH SERVER

Syntax

```
set ssh server hostkey=key-id serverkey=key-id
[expirytime=hours] [logintimeout=seconds]
```

Parameters

hostkey — Specifies the ID number of the encryption key pair to function as the host key.

serverkey — Specifies the ID number of the encryption key pair to function as the server key.

expirytime — Specifies the length of time, in hours, after which the server key pair is regenerated. The range is 0 to 5 hours. Entering 0 never regenerates the key. The default is 0.

logintimeout — Specifies the length of time the server waits before disconnecting an un-authenticated client. The range is 60 to 600 and the default is 180.

Description

This command modifies the configuration of the Secure Shell server parameters.

The HOSTKEY parameter specifies the key ID of the host key pair. The specified key pair must already exist. To create a key pair, refer to “CREATE ENCO KEY” on page 846 (syntax 1).

The SERVERKEY parameter specifies the key of the server key pair. The specified key pair must already exist.

The EXPIRYTIME parameter specifies the time, in hours, after which the Secure Shell server key will expire and will be regenerated. If 0 is specified the key does not expire. The range is 0 to 5 and the default is 0.

The LOGINTIMEOUT parameter specifies the length of time the server waits before disconnecting an un-authenticated client. The range is 60 to 600 seconds. The default is 180 seconds.

Example

The following command sets the Secure Shell server key expiry time to 1 hour:

```
set ssh server expirytime=1
```

SHOW SSH

AlliedWare Plus
Command
Available

Syntax

```
show ssh
```

Parameters

None.

Description

This command displays the current values for the following SSH parameters:

- Versions supported
- Server Status
- Server Port
- Host Key ID
- Host Key Bits (size of host key in bits)
- Server Key ID
- Server Key Bits (size of server key in bits)
- Server Key Expiry (hours)
- Login Timeout (seconds)
- Authentication Available
- Ciphers Available
- MACs Available
- Data Compression

Example

The following command displays the configuration of the Secure Shell server:

```
show ssh
```

AlliedWare Plus Command

Syntax

```
show ssh server
```

Modes

User Exec mode and Privileged Exec mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

```
awplus# show ssh server
```

Chapter 48

TACACS+ and RADIUS Commands

Supported on:

Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	Yes*

(*Stacks do not support the TACACS+ protocol.)

This chapter contains the following commands:

ADD RADIUSSERVER

AlliedWare Plus
Command
Available

Syntax

```
add radiusserver server|ipaddress=ipaddress order=value
[secret=string] [port=value] [accport=value]
```

Parameters

server ***or*** ipaddress
Specifies an IP address of a RADIUS server. The parameters are equivalent.

order
Specifies the order that the RADIUS servers are queried by the switch. This value can be from 1 to 3. The servers are queried starting with 1.

secret
Specifies the encryption key used for this server. The maximum length is 39 characters.

port
Specifies the UDP (User Datagram Protocol) port of the RADIUS server. The default is port 1812.

accport
Specifies the UDP port for RADIUS accounting. The default is port 1813.

Description

This command specifies the IP addresses of the RADIUS servers and the order they are to be queried by the switch. There can be up to three servers, but you can specify only one at a time with this command. You may specify an encryption key, a RADIUS UDP port, and a RADIUS accounting UDP port.

Note
The switch must have a routing interface on the local subnet where the authentication server is a member. The switch uses the IP address of the interface as its source address when sending packets to the server. For instructions on how to add a routing interface to the switch, refer to “ADD IP INTERFACE” on page 708.

Examples

The following command adds a RADIUS server with the IP address 149.245.22.22 and specifies it as the first server in the list:

```
add radiusserver ipaddress=149.245.22.22 order=1
```

The following command adds the RADIUS server with the IP address 149.245.22.22. It specifies the server as the third RADIUS server to be queried by the switch and that it uses the UDP port 3:

```
add radiusserver ipaddress=149.245.22.22 order=3 port=3
```

The following command adds a RADIUS server with an IP address of 149.245.22.22. It specifies the order as 2, the encryption key as tiger74, and the UDP port as 1811:

```
add radiusserver ipaddress=149.245.22.22 order=2
secret=tiger74 port=1811
```

AlliedWare Plus Command

Syntax

`radius-server host` *`ipaddress/order secret/port`*

Mode

Configure mode

Description

You cannot set the UDP port for RADIUS accounting from the AlliedWare Plus commands. To set this parameter, use another management interface, like the standard command line interface.

Example

The following commands add a RADIUS server with the IP address 176.225.15.23 as the second address in the table. The encryption key is abt54 and the UDP port is 1811:

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server host 176.225.15.23/2
abt54/1811
```

ADD TACACSSERVER

AlliedWare Plus Command Available

Syntax

```
add tacacsserver server|ipaddress=ipaddress order=value
[secret=string]
```

Parameters

server ***or*** ipaddress — Specifies the IP address of a TACACS+ server. The parameters are equivalent.

order — Specifies the order the switch queries the TACACS+ servers. The range is 1 to 3. The server assigned the order value of 1 is queried first.

secret — Specifies the optional encryption key used on this server. The maximum length is 39 characters.

Description

This command adds the IP address and encryption key of a TACACS+ server to the switch. This command can also specify the order the TACACS+ servers are queried by the switch. You can add the IP addresses of up to three TACACS+ servers on the AT-9400 Switch. This command can add only one TACACS+ server at a time.

> **Note**
> The switch must have a routing interface on the local subnet where the authentication server is a member. For instructions on how to add a routing interface to the switch, refer to “ADD IP INTERFACE” on page 708.

Examples

The following command adds a TACACS+ server with the IP address 149.245.22.20 and an order value of 1:

```
add tacacsserver ipaddress=149.245.22.20 order=1
```

This command adds a TACACS+ server with an IP address of 149.245.22.24, an order of 2, and an encryption key of lioness54:

```
add tacacsserver ipaddress=149.245.22.24 order=2
secret=lioness54
```

This command adds the IP address 149.245.22.26 as a TACACS+ server and specifies that the server is to be queried third by the switch:

```
add tacacsserver ipaddress=149.245.22.26 order=3
```

AlliedWare Plus Command

Syntax

`tacacs-server host` *`ipaddress order`*

`tacacs-server key` *`secret`*

Mode

Configure mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

This example adds a TACACS+ server with an IP address of 149.11.24.5, an order of 2, and an encryption key of garden124:

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server host 149.11.24.5 2
awplus(config)# tacacs-server key garden124
```

DELETE RADIUSSERVER

AlliedWare Plus Command Available

Syntax

```
delete radiusserver server|ipaddress=ipaddress
```

Parameter

server ***or*** ipaddress	Specifies the IP address of a RADIUS server to be deleted from the management software. The parameters are equivalent.

Description

This command deletes the IP address of a RADIUS server from the management software.

Example

The following command deletes the RADIUS server with the IP address 149.245.22.22:

```
delete radiusserver ipaddress=149.245.22.22
```

AlliedWare Plus Command

Syntax

```
no radius-server host ipaddress
```

Mode

Configure mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example removes the RADIUS server with the IP address 122.34.122.47:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server host 122.34.122.47
```

DELETE TACACSSERVER

AlliedWare Plus Command Available

Syntax

```
delete tacacsserver server|ipaddress=ipaddress
```

Parameter

server ***or*** ipaddress	Specifies the IP address of a TACACS+ server to be deleted from the management software. The parameters are equivalent.

Description

This command is used to remove the IP addresses of TACACS+ servers from the switch. You can remove only one server at a time with this command.

Example

The following command deletes the TACACS+ server with the IP address 149.245.22.20:

```
delete tacacsserver ipaddress=149.245.22.20
```

AlliedWare Plus Command

Syntax

```
no tacacs-server host ipaddress
```

Mode

Configure mode

Description

This AlliedWare Plus command is equivalent to the standard command.

Example

This example removes the TACACS+ server with the IP address 152.112.12.7:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server host 152.112.12.7
```

DISABLE AUTHENTICATION

AlliedWare Plus Command Available

Syntax

```
disable authentication
```

Parameters

None.

Description

This command disables TACACS+ and RADIUS manager account authentication on a switch or stack. When you disable authentication you retain your current authentication parameter settings.

> **Note**
> This command applies only to the TACACS+ and RADIUS manager accounts. Disabling authentication means that you must use the default manager accounts of manager and operator to manage the switch. This command does not affect 802.1x port-based access control.

Example

The following command disables TACACS+ and RADIUS manager account authentication on the switch:

```
disable authentication
```

AlliedWare Plus Command

Syntax

```
login local
```

Mode

Line Console mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example disables manager account authentication on the switch:

```
awplus> enable
awplus# configure terminal
```

```
awplus(config)# line console 0
awplus(config-if)# login local
```

ENABLE AUTHENTICATION

AlliedWare Plus Command Available

Syntax

```
enable authentication
```

Parameters

None.

Description

This command enables TACACS+ or RADIUS manager account authentication on a switch or stack. After you enable manager authentication, you must use the manager accounts you defined on the TACACS+ or RADIUS server to manage the device. To select an authenticator protocol, refer to “SET AUTHENTICATION” on page 893.

Note
If you are using the RADIUS authentication protocol for 802.1x Port-based Network Access Control but not for manager account authentication, you do not need to use this command. Even when the RADIUS manager account feature is disabled, the switch still has access to the RADIUS configuration information for 802.1x port-based access control.

Example

The following command enables manager account authentication:

```
enable authentication
```

AlliedWare Plus Command

Syntax

```
login remotelocal
```

Mode

Line Console mode

Description

This AlliedWare Plus command is identical to the standard command.

Example

This example activates manager account authentication:

```
awplus> enable
awplus# configure terminal
```

```
awplus(config)# line console 0
awplus(config-if)# login remotelocal
```

PURGE AUTHENTICATION

Syntax

```
purge authentication
```

Parameters

None.

Description

This command disables authentication, returns the authentication method to TACACS+, deletes any global secret, and returns the timeout value to its default setting of 10 seconds. This command does not delete the IP addresses or secrets of any RADIUS or TACACS+ authentication servers you may have specified.

Example

The following command returns the authentication settings to their default values:

```
purge authentication
```

SET AUTHENTICATION

AlliedWare Plus
Command
Available

Syntax

```
set authentication method=tacacs|radius [secret=string]
[timeout=value]
```

Parameters

method
Specifies which authenticator protocol, TACACS+ or RADIUS, is to be the active protocol on the switch.

secret
Specifies the global encryption key of the TACACS+ or RADIUS servers. If the servers use different encryption keys, you can leave this parameter blank and set individual encryption keys with “ADD TACACSSERVER” on page 884 or “ADD RADIUSSERVER” on page 882. To remove a previously assigned global key without specifying a new value, enter the string as “none”. The maximum length is 39 characters.

timeout
Specifies the maximum amount of time the switch waits for a response from an authentication server before the switch assumes the server will not respond. If the timeout expires and the server has not responded, the switch queries the next server in the list. After the switch has exhausted the list of servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 300 seconds.

Description

This command selects the authentication protocol. Only one authentication protocol can be active on a switch or stack at a time. You may specify a global encryption code and the maximum number of seconds the switch or stack should wait for a response from an authenticator server.

Examples

The following command selects TACACS+ as the authentication protocol:

```
set authentication method=tacacs
```

The following command selects TACACS+ as the authentication protocol and specifies a global encryption key of tiger54:

```
set authentication method=tacacs secret=tiger54
```

The following command selects RADIUS as the authentication protocol with a global encryption key of leopard09 and a timeout of 15 seconds:

```
set authentication method=radius secret=leopard09 timeout=15
```

The following command removes the current global secret from the RADIUS client without assigning a new value:

```
set authentication method=radius secret=none
```

AlliedWare Plus Command

Syntax

To configure the RADIUS client:

```
radius-server timeout timeout
radius-server key secret
no radius-server timeout
no radius-server key
```

To configure the TACACS+ client:

```
tacacs-server timeout timeout
tacacs-server key secret
no tacacs-server timeout
no tacacs-server key
```

Mode

Configure mode

Description

You cannot specify the authentication method of RADIUS or TACACS+ from the AlliedWare Plus commands.

Example

This example sets the RADIUS timeout to 55 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server timeout 55
```

This example returns the RADIUS timeout parameter to the default value of 30 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server timeout
```

This example sets the RADIUS global encryption key to ‘key22a’:

```
awplus> enable
awplus# configure terminal
awplus(config)# radius-server key key22a
```

This example deletes the current RADIUS global encryption key without defining a new value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no radius-server key
```

This example sets the TACACS+ timeout to 15 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server timeout 15
```

This example returns the TACACS+ timeout parameter to the default value of 30 seconds:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server timeout
```

This example sets the TACACS+ global encryption key to ‘skylight74’:

```
awplus> enable
awplus# configure terminal
awplus(config)# tacacs-server key skylight74
```

This example deletes the current TACACS+ global encryption key without defining a new value:

```
awplus> enable
awplus# configure terminal
awplus(config)# no tacacs-server key
```

SHOW AUTHENTICATION

AlliedWare Plus
Command
Available

Syntax

```
show authentication[=tacacs|radius]
```

Parameters

None.

Description

This command displays the following information about the authenticated protocols:

- Status - The status of your authenticated protocol: enabled or disabled.
- Authentication Method - The active authentication protocol. Either TACACS+ or RADIUS protocol may be active. The TACACS+ protocol is the default.
- The IP addresses of the authentication servers.
- The server encryption keys, if defined.
- TAC global secret - The global encryption code that applies to all authentication servers.
- Timeout - The length of the time, in seconds, before the switch assumes the server will not respond.

Entering the command without specifying either TACACS or RADIUS displays the current status of the authentication feature and the specifics of the currently selected authentication protocol. Specifying TACACS or RADIUS in the command displays the specifics for that authentication protocol.

Example

The following command displays the authentication protocol information:

```
show authentication
```

This command displays the RADIUS client:

```
show authentication=radius
```

This command displays the TACACS+ client:

```
show authentication=tacacs
```

AlliedWare Plus Command

Syntax

To display the RADIUS client:

```
show dot1x statistics
```

To display the TACACS+ client:

```
show tacacs
```

Modes

User Exec mode and Privileged Exec mode

Description

These AlliedWare Plus commands are equivalent to the standard command.

Examples

```
awplus# show dot1x statistics
```

```
awplus# show tacacs
```

Chapter 49

Management Access Control List Commands

Supported on:	
Layer 2+ Models	
AT-9408LC/SP	Yes
AT-9424T/GB	Yes
AT-9424T/SP	Yes
Basic Layer 3 Models	
AT-9424T	Yes
AT-9424T/POE	Yes
AT-9424Ts	Yes
AT-9424Ts/XP	Yes
AT-9448T/SP	Yes
AT-9448Ts/XP	Yes
AT-9400Ts Stacks	

This chapter contains the following commands:

ADD MGMTACL

Syntax

```
add mgmtacl id=value application=telnet|web|ping|all
```

Parameters

id Specifies the identification number of the access control entry (ACE) to be modified. The range is 1 to 256. To view the ID numbers of the existing entries, refer to “SHOW MGMTACL” on page 908.

application Specifies the permitted applications of the ACE. The options are:

telnet Permits Telnet management.

web Permits web browser management.

ping Permits the management workstation to ping the switch.

all Permits all of the above.

You can specify more than one option by separating them with a comma (for example, “Web,Ping”). The new application is added to the existing application of the ACE.

Description

This command modifies the permitted application of an ACE. The new application is added to any application already assigned to the ACE. If you want to assign a new application while overriding the existing one, refer to “SET MGMTACL” on page 907.

Examples

The following command adds web browser as a permitted application to ACE ID 12:

```
add mgmtacl id=12 application=web
```

The following command adds pinging as a permitted application to ACE ID 27:

```
add mgmtacl id=27 application=ping
```

CREATE MGMTACL

Syntax

```
create mgmtacl id=value ipddress=ipaddress mask=string
application=telnet|web|ping|all
```

Parameters

id
: Specifies the identification number for the new access control entry. The range is 1 to 256. Every ACE must have a unique identification number.

ipaddress
: Specifies the IP address of a subnet or a specific management station.

mask
: Specifies the mask used by the switch to filter the IP address. A binary "1" indicates the switch should filter on the corresponding bit of the address, while a "0" indicates that it should not. If, with the IPADDRESS parameter, you specify the IP address of a specific management station, the appropriate mask is 255.255.255.255. If you are filtering on a subnet, then the mask would depend on the address. For example, for a Class C subnet address of 149.11.11.32, the mask would be 255.255.255.224.

application
: Specifies the permitted type of remote management. The options are:

telnet	Permits Telnet management.
web	Permits web browser management.
ping	Permits the management workstation to ping the switch.
all	Permits all of the above.

You can specify more than one option by separating them with a comma (for example, "Web,Ping").

Description

This command creates a new access control entry for the Management ACL. The Management ACL controls who can manage the switch remotely using a web browser or the Telnet application protocol. There can be up to 256 ACEs in a Management ACL.

An ACE is an implicit “permit” statement. A workstation that meets the criteria of the ACE is allowed to remotely manage the switch.

The IPADDRESS parameter specifies the IP address of a specific management station or a subnet.

The MASK parameter indicates the parts of the IP address the switch should filter on. A binary “1” indicates the switch should filter on the corresponding bit of the address, while a “0” indicates that it should not. If you are filtering on a specific IP address, use the mask 255.255.255.255. For a subnet, you need to enter the appropriate mask. For example, to allow all management stations in the subnet 149.11.11.0 to manage the switch, you would enter the mask 255.255.255.0.

The APPLICATION parameter allows you control whether the remote management station can manage the switch using Telnet, a web browser, or both. You can also use it to control whether the workstation can ping the device. For example, you might create an ACE that states that a particular remote management station can only use a web browser to manage the switch.

Note
You must specify all the parameters when creating a new entry.

Examples

The following command creates an ACE that allows the management station with the IP address 169.254.134.247 to manage the switch from either a Telnet or web browser management session and to ping the device:

```
create mgmtacl id=1 ipaddress=169.254.134.247
mask=255.255.255.255 application=all
```

The following command creates an ACE that allows the management station with the IP address 169.254.134.12 to manage the switch with a web browser and to ping the device. However, the workstation cannot manage the switch with the Telnet application protocol:

```
create mgmtacl id=12 ipaddress=169.254.134.12
mask=255.255.255.255 application=web,ping
```

The following command creates an ACE that allows all management stations in the Class A subnet 169.24.144.128 to manage the switch using the Telnet protocol application:

```
create mgmtacl id=17 ipaddress=169.24.144.128
mask=255.255.255.224 application=telnet
```

DESTROY MGMTACL

Syntax

```
destroy mgmtacl id=value
```

Parameters

id Specifies the identification number of the ACE you want to delete. You can delete only one entry at a time.

Description

This command is used to delete ACEs from the Management ACL. You specify the ACEs by their identification numbers, displayed with "SHOW MGMTACL" on page 908.

Note
If you are remotely managing the switch from a Telnet management session and the Management ACL is active, your management session will end and you will be unable to reestablish it should you delete the ACE that specifies your management workstation.

Example

The following command deletes the ACE with the identification number 18 from the Management ACL:

```
destroy mgmtacl id=18
```

DISABLE MGMTACL

Syntax

```
disable mgmtacl
```

Parameters

None

Description

This command disables the Management ACL.

Example

The following command disables the Management ACL:

```
disable mgmtacl
```

ENABLE MGMTACL

Syntax

```
enable mgmtacl
```

Parameters

None.

Description

This command activates the Management ACL.

Note
You will not be able to remotely manage the switch from a Telnet or web browser management session, or ping the device, if you activate the Management ACL before you enter the access control entries (ACEs).

Example

The following command activates the Management ACL:

```
enable mgmtacl
```

PURGE MGMTACL

Syntax

```
purge mgmtacl
```

Parameters

None.

Description

This command deletes all the access control entries from the Management ACL.

> **Note**
> If you delete all the ACEs while remotely managing the unit from a Telnet management session, your management session will end and you will be unable to reestablish it if the Management ACL is active. To continue managing the unit, start a local management session or a remote SSH management session.

Example

The following command deletes all the ACEs from the Management ACL:

```
purge mgmtacl
```

SET MGMTACL

Syntax

```
set mgmtacl id=value [ipaddress=ipaddress] [mask=string]
[application=telnet|web|ping|all]
```

Parameters

id The identification number of the ACE to be modified. To view the ID numbers of the ACEs, refer to "SHOW MGMTACL" on page 908.

ipaddress Specifies a new IP address for the ACE.

mask Specifies a new mask for the ACE.

application Specifies the permitted type of remote management. The options are:

telnet	Permits Telnet management.
web	Permits web browser management.
ping	Permits the management workstation to ping the switch.
all	Permits all of the above.

You can specify more than one option by separating them with a comma (for example, "Web,Ping"). The new application replaces the current permitted application of the ACE.

Description

This command is used to modify the existing management access control entries in the Management ACL. You can use the command to change the IP addresses, subnet masks, or permitted applications of the ACEs.

Examples

This command changes the IP address in ACE ID 22 to 169.254.134.247:

```
set mgmtacl id=22 ipaddress=169.254.134.247
```

This command changes the permitted applications of ACE ID 45 to web browser and pinging:

```
set mgmtacl id=45 application=web,ping
```

SHOW MGMTACL

Syntax

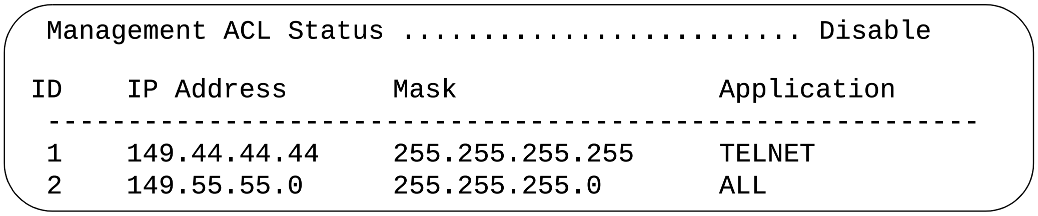
```
show mgmtacl [id=value]
```

Parameters

id Specifies the ID number of an ACE to view.

Description

This command displays the state of the Management ACL and ACL entries. Figure 95 is an example of the information displayed by this command.



```
 Management ACL Status ......................... Disable

ID    IP Address       Mask                 Application
 ----------------------------------------------------------
 1    149.44.44.44     255.255.255.255      TELNET
 2    149.55.55.0      255.255.255.0        ALL
```

Figure 95. SHOW MGMTACL Command with ENTRIES Option

For an explanation of the parameters, refer to “CREATE MGMTACL” on page 901.

Examples

The following command displays the status of all the ACEs in the Management ACL:

```
show mgmtacl
```

The following command displays the details of just ACE ID 14:

```
show mgmtacl id=14
```

Index

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)

(AW = AlliedWare Plus Command)