Management Software

AT-S62

Command Line User's Guide

AT-8516F/SC, AT-8524M, AT-8524POE,
AT-8550GB and AT-8550SP LAYER 2+
FAST ETHERNET SWITCHES

VERSION 1.3.0

Allied Telesyn

PN 613-50486-00 Rev E

Allied Telesyn, 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 Telesyn, 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 Telesyn, Inc. has been advised of, known, or should have known, the possibility of such damages.

Table of Contents

Chapter 10

Chapter 11

Chapter 12

Chapter 13

Chapter 14

Chapter 15

Chapter 30

Chapter 31

Chapter 32

Chapter 33

Chapter 34

Chapter 35

Chapter 36

Chapter 37

Chapter 38

Chapter 39

Preface

This guide describes how to configure an AT-8500 Series switch using the AT-S62 command line interface. The commands are grouped by topic into the following chapters:

- ❑ Chapter 1: Starting a Command Line Management Session on page 16
- ❑ Chapter 2: Basic Command Line Commands on page 20
- ❑ Chapter 3: Enhanced Stacking Commands on page 30
- ❑ Chapter 4: Basic Switch Commands on page 36
- ❑ Chapter 5: Simple Network Time Protocol (SNTP) Commands on page 70
- ❑ Chapter 6: SNMPv1 and SNMPv2 Community Strings and Trap Commands on page 80
- ❑ Chapter 7: SNMPv3 Commands on page 99
- ❑ Chapter 8: Port Parameter Commands on page 157
- ❑ Chapter 9: MAC Address Table Commands on page 177
- ❑ Chapter 10: Port Trunking Commands on page 186
- ❑ Chapter 11: Networking Stack Commands on page 194
- ❑ Chapter 12: LACP Commands on page 204
- ❑ Chapter 13: Port Mirroring Commands on page 219
- ❑ Chapter 14: Statistics Commands on page 223
- ❑ Chapter 15: File System Commands on page 227

A list of the commands appear on the first page of each chapter. The commands are described in alphabetical order.

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 Telesyn sales representative for current information on this product’s export status.

Document Conventions

This document uses the following conventions:

Note
Notes provide additional information.

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

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

Contacting Allied Telesyn

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

Online Support

You can request technical support online by accessing the Allied Telesyn Knowledge Base from the following web site: **www.alliedtelesyn.com/kb**. 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 Support & Services section of the Allied Telesyn web site: **www.alliedtelesyn.com**.

Returning Products

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

To obtain a RMA number, contact Allied Telesyn's Technical Support at our web site: **www.alliedtelesyn.com**.

For Sales or Corporate Information

You can contact Allied Telesyn for sales or corporate information at our web site: **www.alliedtelesyn.com**. To find the contact information for your country, select Contact Us -> Worldwide Contacts.

Management Software Updates

You can download new releases of management software for our managed products from either of the following Internet sites:

- ❑ Allied Telesyn web site: **www.alliedtelesyn.com**
- ❑ Allied Telesyn FTP server: **ftp://ftp.alliedtelesyn.com**

To download new software from the Allied Telesyn FTP server using your workstation's command prompt, you need FTP client software and you must log in to the server. Enter "anonymous" as the user name and your email address for the password.

Chapter 1

Starting a Command Line Management Session

This chapter contains the following topics:

Starting a Management Session

In order to manage an AT-8500 Series switch using command line commands, you must first start a local or Telnet management session. For instructions, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

The default management interface is the command line. The prompt that you will see will differ depending on whether you logged in as Manager or Operator. If you logged in as Manager, you will see "#." If you logged in as Operator, you will see "$." You can now manage the switch with the command line commands.

If you prefer to use the menu interface instead of the command line, type MENU at the command prompt and press Return. To make the menu interface as the default management interface, refer to SET SWITCH CONSOLEMODE on page 28.

Note
Web browser management does not support the command line interface.

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 at any time to see a list of legal next parameters.

❑ Keyword abbreviations - Any keyword can be recognized by typing an unambiguous prefix (for example., “sh” for “show”).

❑ Tab key - Pressing the tab key fills in the rest of a keyword. For example, typing “DI” and pressing the tab key enters “DISABLE.”

Command Formatting

The following formatting conventions are used in this manual:

- ❑ `screen text font` - This font illustrates the format of a command and command examples.
- ❑ *`screen text font`* - Italicized screen text indicates a variable for you to enter.
- ❑ `[ ]` - Brackets indicate optional parameters.
- ❑ | - Bar symbol separates parameter options for you to choose from.

Chapter 2
Basic Command Line Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

CLEAR SCREEN

Syntax

```
clear screen
```

Parameters

None.

Description

This command clears the screen.

Example

The following command clears the screen:

```
clear screen
```

EXIT

Syntax

```
exit
```

Parameters

None.

Description

This command displays the AT-S62 Main Menu. It performs the same function as the MENU command. For instructions on how to use the management menus, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

Example

The following command displays the Main Menu:

```
exit
```

HELP

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
```

LOGOFF, LOGOUT, and QUIT

Syntax

```
logoff
logout
quit
```

Parameters

None.

Description

These three commands perform the same function: they end a management session. If you are managing a slave switch, the commands return you to the master switch from which you started the management session.

Example

The following command ends a management session:

```
logoff
```

MENU

Syntax

```
menu
```

Parameters

None.

Description

This command displays the AT-S62 Main Menu. This command performs the same function as the EXIT command. For instructions on how to use the management menus, refer to the *AT-S62 Management Software Menus Interface User’s Guide*.

Example

The following command displays the AT-S62 Main Menu:

```
menu
```

SAVE CONFIGURATION

Syntax

```
save configuration
```

Parameters

None.

Description

This command saves your changes to the switch's active boot configuration file for permanent storage.

Whenever you make a change to an operating parameter of the switch, such as enter a new IP address or create a new VLAN, the change is stored in temporary memory. It will be lost the next time you reset the switch or power cycle the unit.

To permanently save your changes, you must use this command. The changes are saved in the active boot configuration file as a series of commands. The commands in the file are used by the switch to recreate all of its settings, such as VLANs and port settings, whenever you reset or power cycle the unit.

To view the name of the currently active boot configuration file, see SHOW CONFIG on page 64. To view the contents of a configuration file, see SHOW FILE on page 234. For background information on boot configuration files, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

Example

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

```
save configuration
```

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 double quotes.

Description

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

If you define the system name before you set the command line prompt, the switch uses the system name as the prompt. To set the system name, refer to SET SYSTEM on page 61.

Example

The following command changes the command line prompt to "Sales Switch":

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

SET SWITCH CONSOLEMODE

Syntax

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

Parameter

consolemode	Specifies the mode you want management sessions to start in. Options are:	
	menu	Specifies the AT-S62 Main Menu.
	cli	Specifies the command line prompt. This is the default.

Description

You use this command to specify whether you want your management sessions to start by displaying the command line interface or the AT-S62 Main Menu. The default is the command line interface.

Example

The following command configures the management software to display the menu interface whenever you start a management session:

```
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
Enhanced Stacking Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on enhanced stacking.

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 an AT-8400 Series, AT-8500 Series or AT-8000 Series switch. You can specify the switch by switch number or by MAC address, both of which are displayed with SHOW REMOTELIST on page 35.

Note
You must perform the ACCESS SWITCH command from a management session of a master switch. 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 on page 68.

Note
You must perform the SHOW REMOTELIST command before using 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 return back to the master switch from which you started the management session. For information, refer to LOGOFF, LOGOUT, and QUIT on page 24.

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. Possible settings 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.To view the current enhanced stacking status of a switch, use SHOW SWITCH on page 68.

> **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 either a local or a Telnet management session.

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 a list of the switches in an enhanced stack. This command can only be performed from a management session on a master switch. The list does not include the master switch on which you started the management session.

Note
You must perform the SHOW REMOTELIST command from a management session of a master switch. 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 on page 68.

Example

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=name
```

Chapter 4

Basic Switch Commands

This chapter contains the following commands:

- ❑ DISABLE DHCPBOOTP on page 38
- ❑ DISABLE IP REMOTEASSIGN on page 39
- ❑ DISABLE TELNET on page 40
- ❑ ENABLE BOOTP on page 41
- ❑ ENABLE DHCP on page 42
- ❑ ENABLE IP REMOTEASSIGN on page 43
- ❑ ENABLE TELNET on page 44
- ❑ FORMAT DEVICE on page 45
- ❑ PING on page 47
- ❑ PURGE IP on page 48
- ❑ RESET SWITCH on page 49
- ❑ RESET SYSTEM on page 50
- ❑ RESTART REBOOT on page 51
- ❑ RESTART SWITCH on page 52
- ❑ SET ASYN on page 54
- ❑ SET IP INTERFACE on page 55
- ❑ SET IP ROUTE on page 57
- ❑ SET PASSWORD MANAGER on page 58

❑ SET PASSWORD OPERATOR on page 59

❑ SET SWITCH CONSOLETIMER on page 60

❑ SET SYSTEM on page 61

❑ SET USER PASSWORD on page 62

❑ SHOW ASYN on page 63

❑ SHOW CONFIG on page 64

❑ SHOW DHCPBOOTP on page 65

❑ SHOW IP INTERFACE on page 66

❑ SHOW IP ROUTE on page 67

❑ SHOW SWITCH on page 68

❑ SHOW SYSTEM on page 69

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User’s Guide* for background information on basic switch parameters.

DISABLE DHCPBOOTP

Syntax

```
disable dhcpbootp
```

Parameters

None.

Description

This command deactivates the DHCP and BOOTP client software on the switch. This command is equivalent to DISABLE IP REMOTEASSIGN on page 39. The default setting for the client software is disabled.

To activate the DHCP and BOOTP client software, refer to ENABLE DHCP on page 42, ENABLE BOOTP on page 41, ENABLE IP REMOTEASSIGN on page 43, or SET IP INTERFACE on page 55.

Example

The following command deactivates the DHCP and BOOTP client software:

```
disable dhcpbootp
```

DISABLE IP REMOTEASSIGN

Syntax

```
disable ip remoteassign
```

Parameters

None.

Description

This command deactivates the DHCP and BOOTP client software on the switch. This command is equivalent to DISABLE DHCPBOOTP on page 38. The default setting for the client software is disabled.

To activate the DHCP and BOOTP client software, refer to ENABLE DHCP on page 42, ENABLE BOOTP on page 41, ENABLE IP REMOTEASSIGN on page 43, or SET IP INTERFACE on page 55.

Example

The following command deactivates the DHCP and BOOTP client software:

```
disable ip remoteassign
```

DISABLE TELNET

Syntax

```
disable telnet
```

Parameters

None.

Description

This command disables the Telnet server software on the switch. You might disable the server software if you do not want anyone to manage the switch using the Telnet application protocol or if you plan to use the Secure Shell protocol. The default setting for the Telnet server is enabled.

Example

The following command deactivates the Telnet server:

```
disable telnet
```

ENABLE BOOTP

Syntax

```
enable bootp
```

Parameters

None.

Description

This command activates the BOOTP client software on the switch. This command is equivalent to SET IP INTERFACE on page 55. The default setting for the BOOTP client software is disabled.

Note
When you activate BOOTP, the switch immediately begins to query the network for a BOOTP server. The switch continues to query the network for its IP configuration until it receives a response.

Any static IP address, subnet mask, or gateway address assigned to the switch is deleted from the System Configuration menu and replaced with the value the switch receives from the BOOTP server. If you later disable BOOTP, these values are returned to their default settings.

To disable BOOTP, refer to DISABLE DHCPBOOTP on page 38 or DISABLE IP REMOTEASSIGN on page 39.

Note
You cannot manually assign an IP address or subnet mask to a switch once the BOOTP client software is activated.

Example

The following command activates the BOOTP client software on the switch:

```
enable bootp
```

ENABLE DHCP

Syntax

```
enable dhcp
```

Parameters

None.

Description

This command activates the DHCP client software on the switch. This command is equivalent to ENABLE IP REMOTEASSIGN on page 43 and the SET IP INTERFACE command. The default setting for the DHCP client software is disabled.

Note
When you activate DHCP, the switch immediately begins to query the network for a DHCP server. The switch continues to query the network for its IP configuration until it receives a response.

Any static IP address, subnet mask, or gateway address assigned to the switch is deleted from the System Configuration menu and replaced with the value the switch receives from the DHCP server. If you later disable DHCP, these values are returned to their default settings.

To disable DHCP, refer to DISABLE DHCPBOOTP on page 38 or DISABLE IP REMOTEASSIGN on page 39.

Note
You cannot manually assign an IP address or subnet mask to a switch once the DHCP client software is activated.

Example

The following command activates the DHCP client software on the switch:

```
enable dhcp
```

ENABLE IP REMOTEASSIGN

Syntax

```
enable ip remoteassign
```

Parameters

None.

Description

This command activates the DHCP client software on the switch. This command is equivalent to ENABLE DHCP on page 42. The default setting for the DHCP client software is disabled.

> **Note**
> When you activate DHCP, the switch immediately begins to query the network for a DHCP server. The switch continues to query the network for its IP configuration until it receives a response.
>
> Any static IP address, subnet mask, or gateway address assigned to the switch is deleted from the System Configuration menu and replaced with the value the switch receives from the DHCP server. If you later disable DHCP, these values are returned to their default settings.

To disable DHCP, refer to DISABLE DHCPBOOTP on page 38 or DISABLE IP REMOTEASSIGN on page 39.

> **Note**
> You cannot manually assign an IP address or subnet mask to a switch once the DHCP client software has been activated.

Example

The following command activates the DHCP client software on the switch:

```
enable ip remoteassign
```

ENABLE TELNET

Syntax

```
enable telnet
```

Parameters

None.

Description

This command activates the Telnet server on the switch. With the server activated, you can manage the switch using the Telnet application protocol from any management workstation on your network. To disable the server, refer to DISABLE TELNET on page 40. The default setting for the Telnet server is enabled.

Example

The following command activates the Telnet server:

```
enable telnet
```

FORMAT DEVICE

Syntax

```
format drive=flash
```

Parameter

drive	Specifies the memory device to format. The AT-8500 Series switch supports only one memory device, flash memory.

Description

This command formats the switch's flash memory. It deletes all files in a switch's file system, including configuration files, encryption keys, and event logs, and returns the switch to its factory default settings.

Please note the following before using this command:

- ❑ A switch's IP address and subnet mask, if assigned, are deleted.
- ❑ All port-based and tagged VLANs are deleted.
- ❑ All files in the AT-S62 file system are deleted.
- ❑ All encryption keys stored in the key database are deleted.
- ❑ The current speed setting of the RS232 console port on the switch is retained.
- ❑ To return a switch to its factory default settings without deleting the files in the file system, use the RESTART SWITCH command instead of this command.

⚠ **Caution**
This command results in a switch reset. The switch will not forward traffic while it initializes its operating software, a process that takes approximately 20 seconds to complete. Some network traffic may be lost.

Example

This command deletes all files in the switch's file system and returns the switch to its default factory settings:

```
format drive=flash
```

A confirmation prompt is displayed. Enter **Y** for yes to format the flash memory or **N** for no to cancel the command.

PING

Syntax

```
ping ipaddress
```

Parameter

ipaddress	Specifies the IP address of an end node you want the switch to ping.

Description

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

> **Note**
> The switch must have an IP address and subnet mask in order for you to use this command.

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.

PURGE IP

Syntax

```
purge ip [ipaddress] [netmask] [route]
```

Parameters

ipaddress	Returns the switch's IP address to the default setting 0.0.0.0.
netmask	Returns the subnet mask to the default setting 0.0.0.0.
route	Returns the gateway address to the default setting 0.0.0.0.

Description

This command returns the switch's IP address, subnet mask, and default gateway address to the default settings. This command is similar in function to the RESET IP command. Where they differ is that this command allows you to specify which parameter to reset, while the RESET IP command automatically resets all three parameters.

To set these parameters, refer to SET IP INTERFACE on page 55 and SET IP ROUTE on page 57. To view the current settings, refer to SET SYSTEM on page 61.

Examples

The following command returns the IP address and subnet mask to the default values:

```
purge ip ipaddress netmask
```

The following command resets just the gateway address to its default value:

```
purge ip ipaddress route
```

The following command resets all three parameters:

```
purge ip
```

RESET SWITCH

Syntax

```
reset switch
```

Parameters

None.

Description

This command does all of 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 individual ports, refer to RESET SWITCH PORT on page 165.
- ❑ Resets the statistics counters on all ports to zero. To perform this function on individual ports, refer to RESET SWITCH PORT COUNTER on page 224.
- ❑ Deletes all dynamic MAC addresses from the MAC address table. To perform this function on individual ports, refer to RESET SWITCH FDB on page 181.

Example

This command performs the functions described above:

```
reset switch
```

RESET SYSTEM

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 delete's 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 61. To view the current settings, refer to SHOW SYSTEM on page 69.

Examples

This command deletes all three parameter settings:

```
reset system
```

This command deletes just the name:

```
reset system name
```

RESTART REBOOT

Syntax

```
restart reboot
```

Parameters

None.

Description

This command resets the switch. The switch runs its internal diagnostics, loads the AT-S62 management software, and configures its parameter settings using the current boot configuration file. The reset will takes approximately 20 to 30 seconds to complete. The unit does not forward traffic during the time required to run its internal diagnostics and initialize its operating software. Some network traffic may be lost.

Caution

Be sure to use the SAVE CONFIGURATION command to save your changes before resetting the switch. Any unsaved changes will be discarded.

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

Example

The following command resets the switch:

```
restart reboot
```

RESTART SWITCH

Syntax

```
restart switch config=none|filename.cfg
```

Parameters

config — Specifies a configuration file. The file must already exist on the switch. The value NONE returns the switch to its default values.

Description

This command loads a different configuration file on the switch or returns the switch's parameter settings to their default values.

If you specify a configuration file, the switch automatically resets itself and configures its parameters according to the settings in the configuration file specified in the command. This command does not change the assignment of the active boot configuration file (i.e., the configuration file the switch uses the next time it is reset). If you reset or power cycle the unit, the switch reverts back to its previous configuration. To change the active boot configuration file, refer to SET CONFIG on page 232.

Specifying the NONE parameter returns the switch's operating parameters to the default settings. Please note the following before using this parameter:

- ❑ Returning a switch to its default values deletes all port-based and tagged VLANs you may have created on the switch.
- ❑ This procedure does not delete files from the AT-S62 file system. To delete files, refer to DELETE FILE on page 230.
- ❑ This procedure does not delete encryption keys stored in the key database. To delete encryption keys, refer to DESTROY ENCO KEY on page 512.
- ❑ Returning a switch to its default values does not alter the contents of the active boot configuration file. To reset the active configuration file back to the default settings, you must use Save Configuration command after the switch reboots and you have reestablished your management session. Otherwise the switch will revert back to the previous configuration the next time you reset the unit.

Note
For a list of the default values, refer to Appendix A in the *AT-S62 Management Software Menus Interface User's Guide*.

Note
The switch will not forward traffic during the reset process, which takes 20 to 30 seconds. Some network traffic may be lost.

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

Example

The following command configures the switch using the configuration file SWITCH12.CFG:

```
restart switch config=switch12.cfg
```

The following command resets the switch to its default values:

```
restart switch config=none
```

SET ASYN

Syntax

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

Parameter

speed	Sets the speed of the RS-232 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 the command SET PROMPT on page 27.

Description

This command sets the baud rate of the RS-232 terminal port on the switch. The port is used for local management of the switch. This command can also be used to set the command line prompt.

Note
A change to the baud rate of the port will end 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 RS-232 terminal port on the switch.

Example

This example sets the baud rate to 115200 bps:

```
set asyn speed=115200
```

SET IP INTERFACE

Syntax

```
set ip interface=eth0
ipaddress=ipaddress|dhcp|bootp
mask|netmask=subnetmask
```

Parameters

interface — Specifies the interface number. This value is always "eth0".

ipaddress — Specifies an IP address for the switch or activates the DHCP or BOOTP client software. Options are:

ipaddress — Specifies a static IP address.

DHCP — Activates the DHCP client software.

BOOTP — Activates the BOOTP client software.

mask
netmask — Specifies the subnet mask for the switch. You must specify a subnet mask if you manually assigned the switch an IP address. These parameters are equivalent.

Description

This command configures the following switch parameters:

- ❑ IP address
- ❑ Subnet mask

Note
When setting the IP address and subnet mask of a switch accessed through enhanced stacking, such as a slave switch, you must set the subnet mask first or both IP address and subnet mask simultaneously in the same command. Your network management session will end if you set the IP address without specifying a subnet mask.

This command can also activate the DHCP or BOOTP client software on the switch. Activating DHCP and BOOTP with this command is equivalent to using ENABLE BOOTP on page 41 or ENABLE IP REMOTEASSIGN on page 43.

Note
You cannot manually assign an IP address to the switch if the DHCP or BOOTP client software is activated. To disable the client software, refer to the DISABLE DHCPBOOTP command.

To display the current IP address and subnet mask, refer to SHOW IP INTERFACE on page 66. To return the IP address and subnet mask to their default values, refer to PURGE IP on page 48.

For background information on when to assign a switch an IP address, refer to the *AT-S62 Management Software Menus Interface User's Guide.*

Examples

The following command sets the switch's IP address to 140.35.22.22 and the subnet mask to 255.255.255.0:

```
set ip interface=eth0 ipaddress=140.35.22.22
netmask=255.255.255.0
```

The following command sets just the subnet mask:

```
set ip interface=eth0 netmask=255.255.255.252
```

The following command activates the DHCP client software:

```
set ip interface=eth0 ipaddress=dhcp
```

SET IP ROUTE

Syntax

```
set ip route ipaddress=ipaddress
```

Parameter

ipaddress	Specifies the IP address of the default gateway for the switch.

Description

This command specifies the IP address of the default gateway for the switch. This IP address is required if you intend to remotely manage the device from a remote management station that is separated from the unit by a router.

Example

The following command sets the default gateway to 140.35.22.12:

```
set ip route ipaddress=140.35.22.12
```

SET PASSWORD MANAGER

Syntax

```
set password manager
```

Parameters

None.

Description

This command sets the manager's password. Logging in as manager allows you to view and change all switch parameters. The default password is "friend". A password can be from 1 to 16 alphanumeric characters. Allied Telesyn recommends avoiding special characters, such as spaces, asterisks or exclamation points, since some web browsers do not accept them in passwords. A password is case sensitive.

Example

The following command changes the manager's password:

```
set password manager
```

Follow the prompts to enter the new password.

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 1 to 16 alphanumeric characters. Allied Telesyn recommends avoiding special characters, such as spaces, asterisks or exclamation points, since 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.

SET SWITCH CONSOLETIMER

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. If the AT-S62 software does not detect any activity from a local or remote management station after the period of time set by the console timer, it automatically ends the management session. 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 on page 68.

Example

The following command sets the console timer to 25 minutes:

```
set switch consoletimer=25
```

SET SYSTEM

Syntax

```
set system [name=”name”] [contact=”contact”]
[location=”location”]
```

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.

Description

This command sets a switch’s name, the name of the network administrator responsible for managing the unit, and the location of the unit.

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 69. To delete a value without assigning a new value, refer to RESET SYSTEM on page 50.

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”
```

SET USER PASSWORD

Syntax

```
show user manager|operator password=password
```

Parameter

password	Specifies the new manager or operator password.

Description

This command changes the passwords for the manager and operator accounts. The default password for the manager account is “friend.” The default for the operator account is “operator.”

A password can be from 1 to 16 alphanumeric characters. Allied Telesyn recommends avoiding special characters, such as spaces, asterisks or exclamation points, since some web browsers do not accept them in passwords. The password is case sensitive.

This command is equivalent to SET PASSWORD MANAGER on page 58 and SET PASSWORD OPERATOR on page 59.

Example

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

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

SHOW ASYN

Syntax

```
show asyn
```

Parameters

None.

Description

This command displays the settings for the RS-232 Terminal Port on the switch. To adjust the baud rate, which is the only setting on the port you can change, refer to SET ASYN on page 54.

Example

The following command displays the RS-232 Terminal Port settings:

```
show asyn
```

SHOW CONFIG

Syntax

```
show config [dynamic] [info]
```

Parameters

dynamic	Displays the settings for all the switch and port parameters in their equivalent command line commands.
info	Displays all switch settings.

Description

This command, when used without any 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 whenever you use the SAVE CONFIGURATION command. To change the boot configuration file, refer to SET CONFIG on page 232.

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.

The DYNAMIC parameter displays the equivalent command line commands for those switch parameters that have been changed from their default settings.

The INFO parameter displays all the switch settings. It performs the same function as all the other SHOW commands in one command.

Example

The following command displays the names of the current configuration files:

```
show config
```

This command displays all the switch settings:

```
show config info
```

SHOW DHCPBOOTP

Syntax

```
show dhcpbootp
```

Parameters

None.

Description

This command displays the status of the DHCP and BOOTP client software on the switch. If neither is activated, the status will be "disabled." The default setting is disabled.

To enable the DHCP and BOOTP client software, refer to ENABLE BOOTP on page 41, ENABLE DHCP on page 42, or ENABLE IP REMOTEASSIGN on page 43. To disable the client software, refer to DISABLE DHCPBOOTP on page 38 or DISABLE IP REMOTEASSIGN on page 39.

Example

The following command displays the status of the DHCP and BOOTP client software:

```
show dhcpbootp
```

SHOW IP INTERFACE

Syntax

```
show ip interface=eth0
```

Parameters

interface Specifies the switch’s interface number. This value is always “eth0”.

Description

This command displays the current values for the following switch parameters:

- ❑ IP address
- ❑ Subnet mask
- ❑ Default gateway

To manually set the IP address and subnet mask, refer to SET IP INTERFACE on page 55. To manually set the default gateway address, refer to SET IP ROUTE on page 57.

Example

The following command displays the IP address, subnet mask, and default gateway of the switch:

```
show ip interface=eth0
```

SHOW IP ROUTE

Syntax

```
show ip route
```

Parameters

None.

Description

This command displays the switch's default gateway address. You can also display the gateway address using SHOW IP INTERFACE on page 66.

To manually set the default gateway address, refer to SET IP ROUTE on page 57.

Example

The following command displays the default gateway address of the switch:

```
show ip route
```

SHOW SWITCH

Syntax

```
show switch
```

Parameters

None.

Description

This command displays the following switch parameters:

- ❑ Application software version
- ❑ Application software build date
- ❑ Bootloader version
- ❑ Bootloader build date
- ❑ MAC address
- ❑ Switch VLAN mode
- ❑ Management VLAN
- ❑ Ingress filtering
- ❑ Enhanced stacking mode
- ❑ Management disconnect timer interval
- ❑ Web server status
- ❑ Telnet server status
- ❑ MAC address aging time
- ❑ Console startup mode
- ❑ Management VLAN ID
- ❑ Port mirroring

Example

The following command displays the switch information listed above:

```
show switch
```

SHOW SYSTEM

Syntax

```
show system
```

Parameters

None.

Description

This command displays the following information:

- ❑ MAC address
- ❑ Model name
- ❑ Serial number
- ❑ IP address
- ❑ Subnet mask
- ❑ Gateway address
- ❑ System operating time
- ❑ Application software version and build date
- ❑ Bootloader version and build date
- ❑ Switch name, administrator, and location
- ❑ Power status

Example

The following command displays the above information:

```
show system
```

Chapter 5

Simple Network Time Protocol (SNTP) Commands

This chapter contains the following commands:

- ❑ ADD SNTPSERVER PEER|IPADDRESS on page 71
- ❑ DELETE SNTPSERVER PEER|IPADDRESS on page 72
- ❑ DISABLE SNTP on page 73
- ❑ ENABLE SNTP on page 74
- ❑ PURGE SNTP on page 75
- ❑ SET DATE TIME on page 76
- ❑ SET SNTP on page 77
- ❑ SHOW SNTP on page 78
- ❑ SHOW TIME on page 79

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on SNTP.

ADD SNTPSERVER PEER|IPADDRESS

Syntax

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

Parameter

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

Description

This command adds the IP address of an SNTP server to the SNTP client software on the switch. The switch uses the SNTP server to set its date and time. If an IP address has already been assigned, the new address overwrites the old address. To view the current SNTP client settings, refer to SHOW SNTP on page 78.

Note
If the switch is obtaining 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
```

DELETE SNTPSERVER PEER|IPADDRESS

Syntax

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

Parameter

peer 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 78.

Example

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

```
delete sntpserver ipaddress=148.35.16.248
```

DISABLE SNTP

Syntax

```
disable sntp
```

Parameters

None.

Description

This command disables the SNTP client software on the switch. The default setting for SNTP is disabled.

Example

The following command disables SNTP on the switch:

```
disable sntp
```

ENABLE SNTP

Syntax

```
enable sntp
```

Parameters

None.

Description

This command enables the SNTP client software on the switch. The default setting for SNTP is disabled. Once enabled, the switch will obtain its date and time from an SNTP server, assuming that you have specified a server IP address with ADD SNTPSERVER PEER|IPADDRESS on page 71.

Example

The following command enables the SNTP client software:

```
enable sntp
```

PURGE SNTP

Syntax

```
purge sntp
```

Parameters

None.

Description

This command disables the SNTP client software and returns its parameters to the default values.

Example

The following command resets SNTP:

```
purge sntp
```

SET DATE TIME

Syntax

```
set date=dd-mm-yyyy time=hh:mm:ss
```

Parameter

date	Specifies the date for the switch in day-month-year format.
time	Specifies the hour, minute, and second for the switch's time in 24-hour format.

Description

This command sets the date and time on the switch. You can use this command to set the switch's date and time if you are not using an SNTP server. To view the current time, refer to SHOW TIME on page 79.

> **Note**
> The system's date and time, when set with this command, are lost whenever you power cycle or reset the switch. To avoid having to reenter the date and time, you can configure the SNTP client software so that the switch automatically obtains this information from an SNTP server.

Example

The following command sets the switch's date to March 11, 2004 and the time to 4:34 pm and 52 seconds:

```
set date=11-03-2004 time=16:34:52
```

The following command sets just the date to April 2, 2004:

```
set date=02-04-2004
```

SET SNTP

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 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 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, this option should be set 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
```

SHOW SNTP

Syntax

```
show sntp
```

Parameters

None.

Description

This command displays the following information:

- ❑ Status of the SNTP client software
- ❑ SNTP server IP address
- ❑ UTC Offset
- ❑ Daylight Savings Time (DST) - enabled or disabled
- ❑ Poll interval
- ❑ Last Delta - The last adjustment that had to be 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
```

SHOW TIME

Syntax

```
show time
```

Parameters

None.

Description

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

Example

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

```
show time
```

Chapter 6

SNMPv1 and SNMPv2 Community Strings and Trap Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on SNMP.

ADD SNMP COMMUNITY

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 workstation to have SNMP access to the switch using the community string.

Description

This command adds the IP address of a trap receiver or a management station to an existing community string.

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 83. To view the current community strings, refer to SHOW SNMP on page 97.

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
```

CREATE SNMP COMMUNITY

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 characters. Spaces are allowed. The name must be enclosed in double quotes if it includes a space or 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 values are:

yes, on, true The community string is open, meaning any management workstation can use the string to access the switch. These values are equivalent.

no, off, false The community string is closed, meaning only those management workstations 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 workstations, 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 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 workstation 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 workstations whose IP addresses are assigned to the community string will be able to use it to manage the switch. 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 81.

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 workstations 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 81.

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 workstation that will use the string:

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

(The OPEN=NO parameter could be omitted from the example since 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
```

DELETE SNMP COMMUNITY

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 a community string.

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 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
```

DESTROY SNMP COMMUNITY

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 an SNMP community string from the switch. IP addresses of management stations and SNMP trap receivers assigned to the community string are deleted as well.

Example

The following command deletes the community string “wind44”:

```
destroy snmp community=wind44
```

DISABLE SNMP

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.

Example

The following command disables SNMP on the switch:

```
disable snmp
```

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 enabled.

The AUTHENTICATETRAP and AUTHENTICATE_TRAP keywords are equivalent.

To activate the authentication failure trap, refer to ENABLE SNMP AUTHENTICATETRAP on page 93

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 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 workstation 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

Syntax

```
enable snmp
```

Parameters

None.

Description

This command activates SNMP on the switch. Once activated, you can remotely manage the unit with an SNMP application program from a management station on your network. The default setting for SNMP on the switch is disabled.

Example

The following command activates SNMP on the switch:

```
enable snmp
```

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 81 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"
```

Parameters

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 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 community string is enabled. You would use this command to enable a community string that you had 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]
```

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 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 The community string is open, meaning that any management workstation can use the string to access the switch.

no The community string is closed, meaning that only those management workstations whose IP addresses are assigned to the string can use it to access the switch. To add IP addresses of management workstations to a community string, refer to ADD SNMP COMMUNITY on page 81. The default setting for a community string is closed.

Description

This command changes the access level or 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

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 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 92. To disable SNMP, refer to DISABLE SNMP on page 89.
- ❑ 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 93. To disable the sending of this trap, see DISABLE SNMP AUTHENTICATETRAP on page 90. To add IP addresses of management stations to receive the trap, refer to the ADD SNMP COMMUNITY on page 81.
- ❑ 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 83. To delete community strings, refer to DESTROY SNMP COMMUNITY on page 88.

- ❑ 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 81. To delete addresses, refer to DELETE SNMP COMMUNITY on page 86.

- ❑ 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 81. To delete addresses, refer to DELETE SNMP COMMUNITY on page 86.

- ❑ Access Status - If a community string shows an Open Access with Yes, the string has an open access status, meaning any management workstations can use the string. A string with a Open Access of No has a closed access status; only those management workstations whose IP addresses have been assigned to the string can use it. To change the access status, refer to SET SNMP COMMUNITY on page 95.

Examples

The following command displays the SNMP status and 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 workstations that can use the string and the IP addresses of SNMP trap receivers:

```
show snmp community=private
```

Chapter 7

SNMPv3 Commands

This chapter contains the following commands:

- ❑ DESTROY SNMPv3 TARGETADDR on page 130
- ❑ DESTROY SNMPv3 TARGETPARMS on page 131
- ❑ DESTROY SNMPV3 VIEW on page 132
- ❑ SET SNMPV3 ACCESS on page 133
- ❑ SET SNMPV3 COMMUNITY on page 135
- ❑ SET SNMPV3 GROUP on page 137
- ❑ SET SNMPV3 NOTIFY on page 139
- ❑ SET SNMPV3 TARGETADDR on page 141
- ❑ SET SNMPV3 TARGETPARAMS on page 143
- ❑ SET SNMPV3 USER on page 145
- ❑ SET SNMPV3 VIEW on page 147
- ❑ SHOW SNMPV3 ACCESS on page 149
- ❑ SHOW SNMPV3 COMMUNITY on page 150
- ❑ SHOW SNMPv3 GROUP on page 151
- ❑ SHOW SNMPV3 NOTIFY on page 152
- ❑ SHOW SNMPV3 TARGETADDR on page 153
- ❑ SHOW SNMPV3 TARGETPARAMS on page 154
- ❑ SHOW SNMPV3 USER on page 155
- ❑ SHOW SNMPV3 VIEW on page 156

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the SNMPv3 protocol.

ADD SNMPV3 USER

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

The following command creates an SNMPv3 user with the name “steven142” with 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
```

The following 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
```

CLEAR SNMPV3 ACCESS

Syntax

```
clear snmpv3 access=access
[securitymodel=v1|v2c|v3]
[securitylevel=noauthentication|authentication|
privacy] readview writeview notifyview
```

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 security group to view the information specified by the View Table entry. This is an optional parameter.

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.

notifyview	Specifies a Notify View Name that allows the users assigned to this security group to send traps permitted in the specified View. This is an optional parameter.

Description

This command clears the specified fields in an SNMPv3 Access Table entry.

Examples

The follow command clears the readview parameter in a security group called “Engineering” which has a security model of the SNMPv3 protocol and a security level of privacy.

```
clear snmpv3 access=Engineering securitymodel=v3
securitylevel=privacy readview
```

The follow command clears the values in the readview, writeview, and notifyview parameters in a security group called “SystemTest.” This group has a security model of the SNMPv3 protocol and a security level of authentication.

```
clear snmpv3 access=SystemTest securitymodel=v3
securitylevel=authentication readview writeview
notifyview
```

CLEAR SNMPV3 COMMUNITY

Syntax

```
clear snmpv3 community index=index transporttag
```

Parameters

index	Specifies the name of an existing SNMPv3 Community Table entry, up to 32 alphanumeric characters.
transporttag	Specifies the transport tag, up to 32 alphanumeric characters.

Description

This command clears the transporttag parameter in an SNMPv3 Community Table entry.

Examples

The following command clears the value of the transporttag parameter in the SNMPv3 Community Table entry with an index of 1005.

```
clear snmpv3 community index=1005 transporttag
```

The following command clears the value of the transporttag parameter in the SNMPv3 Community Table entry with an index of 421.

```
clear snmpv3 community index=421 transporttag
```

CLEAR SNMPV3 NOTIFY

Syntax

```
clear snmpv3 notify=notify tag
```

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.

Description

This command clears the value of the tag parameter in an SNMPv3 Notify Table entry.

Examples

The following command deletes the value of the tag parameter in an SNMPv3 Notify Table entry called “hwengtrap.”

```
clear snmpv3 notify=hwengtraptag tag
```

The following command deletes the value of the tag parameter in an SNMPv3 Notify Table entry called “hwenginformtag.”

```
clear snmpv3 notify=hwenginform tag
```

CLEAR SNMPV3 TARGETADDR

Syntax

```
clear snmpv3 targetaddr=targetaddr taglist
```

Parameters

targetaddr	Specifies the name of the SNMPv3 Target Address Table entry, up to 32 alphanumeric characters.
taglist	Specifies a tag or list of tags, up to 256 alphanumeric characters.

Description

This command clears the value of the taglist parameter in an SNMPv3 Target Address Table entry.

Examples

The following command deletes the value of the taglist parameter from the SNMPv3 Target Address Table entry called "snmphost79."

```
clear snmpv3 targetaddr=snmphost44 taglist
```

The following command deletes the value of the taglist parameter from the SNMPv3 Target Address Table entry called "snmphost79."

```
clear snmpv3 targetaddr=snmphost79 taglist
```

CLEAR SNMPV3 VIEW

Syntax

```
clear snmpv3 view=view [subtree=OID|text] mask
```

Parameters

view	Specifies the name of the SNMPv3 view, up to 32 alphanumeric characters.	
subtree	Specifies the view of the MIB Tree. Options are:	
	OID	A numeric value in hexadecimal format.
	text	Text name of the view.
mask	Specifies the subtree mask, in hexadecimal format.	

Description

This command clears the value of the mask parameter in an SNMPv3 View Table entry.

Examples

The following command clears the value of the subtree mask from the SNMPv3 view of 1.3.6.1.2.1.1.

```
clear snmpv3 view=1.3.6.1.2.1.1 mask
```

The following command clears the value of subtree mask from the SNMPv3 view called private. The subtree has a value of 1.3.6.1.4 (private MIBs).

```
clear snmpv3 view=private subtree=1.3.6.1.4 mask
```

CREATE SNMPV3 ACCESS

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 an SNMPv3 Access Table entry.

Examples

In the following command, a security group is created 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
```

In the following command, a security group is created 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
```

In the following command, a security group is created 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.

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 109.

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.

Example

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

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

In the following command, the SNMPv3 Notify Table entry is 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
```

In the following command, the SNMPv3 Notify Table entry is 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
```

CREATE SNMPV3 TARGETADDR

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
```

CREATE SNMPV3 TARGETPARAMS

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. 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 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
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
securitylevel=authentication
storagetype=nonvolatile
```

CREATE SNMPV3 VIEW

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
```

DELETE SNMPV3 USER

Syntax

```
delete snmpv3 user=user
```

Parameters

user	Specifies the name of an SNMPv3 user to delete from the switch.

Description

This command deletes an SNMPv3 User Table entry. 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
```

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

Syntax

```
destroy snmpv3 notify=notify
```

Parameter

notify	Specifies an SNMPv3 Notify Table entry.

Description

This command deletes an SNMPv3 Notify Table entry. 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
```

DESTROY SNMPv3 TARGETADDR

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.

Examples

The following command deletes an SNMPv3 Address Table entry called “snmpv3host77.”

```
destroy snmpv3 targetaddr=snmpv3host77
```

Examples

The following command deletes an SNMPv3 Address Table entry called “snmpmanager.”

```
destroy snmpv3 targetaddr=snmpmanager
```

DESTROY SNMPv3 TARGETPARMS

Syntax

```
destroy snmpv3 targetparams=targetparams
```

Parameter

targetparams	Specifies an SNMPv3 Target Parameters table entry.

Description

This command deletes an SNMPv3 Target Parameters Table entry. After you delete an SNMPv3 Target Parameters Table entry, you cannot recover it.

Examples

The following command deletes the SNMPv3 Target Parameters Table entry called “targetparameter1.”

```
destroy snmpv3 targetparams=targetparameter1
```

The following command deletes the SNMPv3 Target Parameters Table entry called “snmpmanager.”

```
destroy snmpv3 targetparams=snmpmanager
```

DESTROY SNMPV3 VIEW

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 an SNMPv3 View Table entry. After you delete an SNMPv3 View Table entry, you cannot recover it.

Examples

In the following command, the SNMPv3 View Table entry named experimental is deleted. The subtree value of this table entry is experimental.

```
destroy snmpv3 view=experimental
subtree=experimental
```

In the following command, the SNMPv3 View Table entry named directory is deleted. The subtree value of this table entry is 1.3.6.1.3.

```
destroy snmpv3 view=directory subtree=1.3.6.1.3
```

SET SNMPV3 ACCESS

```
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

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
```

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

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 the SNMPv3 Notify Table entry called “testengtrap1”:

```
show snmpv3 notify=testengtrap1
```

The following command displays all of the SNMPv3 Notify Table entries:

```
show snmpv3 notify
```

SHOW SNMPV3 TARGETADDR

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
```

SHOW SNMPV3 TARGETPARAMS

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 SNMPv3 Target Parameters Table entry called “snmpv3manager95”:

```
show snmpv3 targetparams=snmpv3manager95
```

The following command displays all of the SNMPv3 Target Parameters Table entries:

```
show snmpv3 targetparams
```

SHOW SNMPV3 USER

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 example displays the SNMPv3 User Table entry for a user name of Robert:

```
show snmpv3 user=Robert
```

The following example displays all of the SNMPv3 User Table entries:

```
show snmpv3 user
```

SHOW SNMPV3 VIEW

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 targetparams=snmpv3manager95
```

The following command displays all the SNMPv3 View Table entries:

```
show snmpv3 targetparams
```

Chapter 8
Port Parameter Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the port parameters.

ACTIVATE SWITCH PORT

Syntax

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

Parameter

port	Specifies a port. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

If a port is using Auto-Negotiation to set its speed and duplex mode, this command prompts the port to renegotiate its settings with its end node. This can be useful if you believe a port and an end node have not successfully negotiated their settings.

If the speed and duplex mode on a port were set manually, this command overrides those settings and returns the port to Auto-Negotiation. It should be noted that when a port is returned to Auto-Negotiation, the MDI/MDI-X setting on the port is returned to Auto-Detect.

Example

This command forces ports 1 and 4 to use Auto-Negotiation to set speed and duplex mode:

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

DISABLE INTERFACE LINKTRAP

Syntax

```
disable interface=port linktrap
```

Parameter

port	Specifies the port where you want to disable SNMP link traps. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command disables 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
```

DISABLE SWITCH PORT

Syntax

```
disable switch port=port
```

Parameter

port	Specifies the port to disable. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command disables a port. Once disabled, a port stops forwarding traffic. The default setting for a port is enabled. This command performs the same function are the STATUS parameter in the SET SWITCH PORT command.

Example

The following command disables ports 12 and 24:

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

DISABLE SWITCH PORT FLOW

Syntax

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

Parameter

port	Specifies the port where you want to deactivate flow control. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command deactivates flow control on a port. Flow control applies only to ports operating in full duplex mode. This command performs the same function as the FLOWCONTROL parameter in the SET SWITCH PORT command.

Example

This command deactivates flow control on port 6:

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

ENABLE INTERFACE LINKTRAP

Syntax

```
enable interface=port linktrap
```

Parameter

port	Specifies the port on which you want to enable SNMP link traps. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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

Example

The following command enables SNMP link traps on port 21:

```
enable interface=21
```

ENABLE SWITCH PORT

Syntax

```
enable switch port=port
```

Parameter

port

Specifies the port to enable. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command enables a port. Once enabled, a port begins to forward traffic. The default setting for a port is enabled. This command performs the same function are the STATUS option is the SET SWITCH PORT command.

Example

The following command enables ports 1 to 4:

```
disable switch port=1-4
```

ENABLE SWITCH PORT FLOW

Syntax

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

Parameter

port Specifies the port where you want to activate flow control. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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 a PAUSE packet whenever it wants the end node to stop sending packets.

This command performs the same function as the FLOWCONTROL option in the SET SWITCH PORT command.

Example

This command activates flow control on port 5:

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

RESET SWITCH PORT

Syntax

```
reset switch port=port
```

Parameter

port	Specifies the port to reset. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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. This command performs the same function as the SOFTRESET parameter in the SET SWITCH PORT command.

Example

The following command resets ports 5 to 8:

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

SET SWITCH PORT

Syntax

```
set switch port=port [description="description"]
[status=enabled|disabled]
[speed=autonegotiate|10mhalf|10mfull|10mhauto|10m
fauto|100mhalf|100mfull|100mhauto|100mfauto|1000m
full|1000mfauto]
[mdimode=mdi|mdix|auto]
[flowcontrol=disable|enable|auto]
[fctrllimit=auto|value]
[backpressure=yes|no|on|off|true|false|enabled|
disabled]
[bplimit=auto|value]
[bcastfiltering=yes|no|on|off|true|false|enabled|
disabled]
[holbplimit=value]
[renegotiation=auto]
[softreset]
[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. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

description — Specifies a name or description for the port. The name can be from one to fifteen alphanumeric characters. Spaces are allowed, but you should not use special characters, such as asterisks or exclamation points. If the name contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

status — Specifies the operating status of the port. Possible settings are:

enabled — The port forwards Ethernet frames. This is the default setting.

disabled — The port does not forward frames.

speed — Sets the speed and duplex mode of the port. Settings for this parameter are:

autonegotiate	The port Auto-Negotiates both speed and duplex mode.This is the default setting.
10mhalf	10 Mbps and half-duplex mode.
10mfull	10 Mbps and full-duplex mode.
10mhauto	10 Mbps and half-duplex mode with Auto-Negotiation.
10mfauto	10 Mbps and full-duplex mode with Auto-Negotiation.
100mhalf	100 Mbps and half-duplex mode.
100mfull	100 Mbps and full-duplex mode.
100mhauto	100 Mbps and half-duplex mode with Auto-Negotiation.
100mfauto	100 Mbps and full-duplex mode with Auto-Negotiation.
1000mfull	1000 Mbps and full-duplex mode.
1000mfauto	1000 Mbps and full-duplex mode with Auto-Negotiation.

Note
The selections 10mfauto, 100mhauto, 100mfauto, and 1000mfauto cause a port to Auto-Negotiate to a lower speed and/or to half duplex mode if required by the end node.

mdimode — Sets the wiring configuration of the port. This parameter applies only to twisted pair ports. You cannot change the MDI/MDIX setting when a port's speed is set to Auto-Negotiate. Possible values are:

mdi	Sets the port's configuration to MDI.
mdix	Sets the port's configuration to MDI-X.
auto	Automatically sets the port's wiring configuration to either MDI or MDI-X, depending on the end node connected to the port. This is the default setting.

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. Possible values are:

disabled	No flow control.

enabled	Flow control is activated.

auto	The switch sets flow control to match flow control on the end node connected to the port. If the end node is using flow control, the switch port also uses flow control. If the end node is not using flow control, neither will the switch port.

fctrllimit	Specifies the number of cells for flow control. A cell represents 64 bytes. The range is 1 to 57,344 cells. The default is 57,344 cells.

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

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

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

bplimit	Specifies the number of cells for backpressure. A cell represents 64 bytes. The range is 1 to 57,344 cells. The default is 57,344 cells.

bcastfiltering	Controls the broadcast filter. These parameters are equivalent. Possible values are:

yes, on, true, enabled	The port forwards broadcast frames. These values are equivalent.

no, off, false, disabled	The port discards all ingress broadcast frames. These values are equivalent.

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 64 bytes. The range is 1 to 61,440 cells; the default is 58,000.

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 value is:

auto   Renegotiates with the end node speed and duplex mode.

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

priority   Specifies the port's 802.1p priority level. The priority level determines the priority queue on the egress port used to store untagged packets and, if the OVERRIDEPRIORITY parameter is included, tagged packets. There are eight priority levels, 0 to 7 with 0 the lowest priority. Each port has four egress queues. Table 1 lists the default mappings between the priority levels and the egress queues:

Table 1 Default Mappings of IEEE 802.1p Priority Levels to Egress Queues

IEEE 802.1p Priority Level	Port Egress Queue
0 or 1	Q0 (lowest)
2 or 3	Q1
4 or 5	Q2
6 or 7	Q3 (highest)

overridepriority   Determines if a port should ignore the priority level in tagged packets and store the packets in the egress port's priority queue that corresponds to the priority level set with the PRIORITY parameter. Possible values are:

yes, on, true   Overrides the priority level in tagged packets. The values are equivalent.

no, off, false   Does not override the priority in tagged packets. The values are equivalent.

Description

This command sets a port's operating parameters. You can set more than one parameter at a time. For an explanation of the port parameters, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

To configure the fiber optic port on a GBIC or SFP module in Port 49 or 50 of an AT-8550GB or AT-8550SP switch, the port must have a valid connection to an end node. Otherwise, specifying Ports 49 and 50 configure the twisted pair ports 49R and 50R.

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 to 100 Mbps, the duplex mode to full duplex, the wiring configuration to MDI-X, and flow control to enabled for ports 2 to 6:

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

The following command sets port priority to 5 and activates the broadcast filter for ports 5, 8, and 12:

```
set switch port=5,8,12 priority=5
bcastfiltering=enabled
```

The following command resets port 5:

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

SET SWITCH PORT RATELIMIT

Syntax

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

Parameters

port — Specifies all ports on the switch. This feature cannot be configured on a per-port basis. You must specify ALL.

rate — Specifies the number of ingress packets the switch ports accept each second. This setting applies all packet types that have their rate limit enabled. The range is 0 to 262,143.

bcastratelimiting — Enables or disables rate limiting for ingress broadcast packets. Settings for this parameter are:

yes, on, true, enabled	Activates broadcast packet rate limit on the port. The values are equivalent.
no, off, false, disabled	Deactivates broadcast packet rate limit on the port. The values are equivalent.

mcastratelimiting — Enables or disables rate limiting for ingress multicast packets. Settings for this parameter are:

yes, on, true, enabled	Activates multicast packet rate limit on the port. The values are equivalent.
no, off, false, disabled	Deactivates multicast packet rate limit on the port. The values are equivalent.

unkucastratelimiting — Enables or disables rate limiting for unknown ingress unicast packets. An unknown unicast packet is a packet whose destination MAC address is not stored in the switch's MAC address table. Settings for this parameter are:

yes, on, true, enabled	Activates unknown unicast packet rate limit on the port. The values are equivalent.
no, off, false, disabled	Deactivates unknown unicast packet rate limit on the port. The values are equivalent.

Description

This command sets the maximum number of ingress multicast, broadcast, and unknown unicast packets the switch ports accept each second. Packets exceeding the threshold are discarded. You can enable the rate limiting threshold independently for each packet type. However, the same threshold applies to all packet types.

The RATE parameter sets the packet limit. This limit applies to all the ports. There can be only one packet limit value for the switch. Additionally, the same packet limit applies to the three types of packets that you can filter on.

The other parameters are used to toggle on and off the different filters. A filter applies to all switch ports.

Here is an example. Assume that you set a rate limit of 5,000 packets and you enable multicast and broadcast rate limiting. Each switch port will accept up to 5,000 multicast packets and 5,000 broadcast packets each second. If a port receives more than that of either type, it discards the extra packets. Because the feature was not activated for unknown unicast packets, their number is not restricted.

Examples

The following command sets a rate limit of 40,000 ingress packets and activates broadcast and multicast rate limiting on all switch ports:

```
set switch port=all rate=40000
bcastratelimiting=enabled
mcastratelimiting=enabled
```

The following command activates unicast rate filtering on all ports without changing the current rate limit:

```
set switch port=all unkucastratelimiting=enabled
```

This command changes the rate limit to 15,000 packets:

```
set switch port=all rate=15000
```

The following command deactivates unicast rate filtering on all ports:

```
set switch port=all unkucastratelimiting=disabled
```

SHOW INTERFACE

Syntax

```
show interface=port
```

Parameter

port	Specifies the port whose interface information you want to display. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command displays the contents of the interface MIB for a port and provides the following information:

- ❑ ifIndex - The port number.
- ❑ ifMTU - The size, in octets, of the largest packet that can be transmitted on this port.
- ❑ ifSpeed - An estimate of the port's current bandwidth, in bits per second.
- ❑ ifAdminStatus - The configured state of the port, one of the following:

  up - The port is enabled.

  down - The port has been manually disabled.
- ❑ 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. The switch sends an SNMP link trap whenever there is a change to the status of the link on the port. To disable link traps, see DISABLE INTERFACE LINKTRAP on page 159.

  disabled - Link traps are disabled. To enable link traps, see ENABLE INTERFACE LINKTRAP on page 162.

Example

The following command displays the above information on port 21:

```
show interface=21
```

SHOW SWITCH PORT

Syntax

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

Parameter

port	Specifies the port whose parameter settings you want to view. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22). All ports are displayed if you omit the port number.

Description

This command displays a port’s operating parameters, such as speed and duplex mode. Refer to the *AT-S62 Management Software Menus Interface User’s Guide* for details on port parameters.

A GBIC or SFP module in Port 49 or 50 of an AT-8550GB or AT-8550SP switch must have a valid connection to an end node in order for you to view its parameter settings. Otherwise, specifying Ports 49 and 50 display the parameter settings of the twisted pair ports 49R and 50R.

Examples

The following command displays the operating settings for all ports:

```
show switch port
```

The following command displays the operating settings for port 14:

```
show switch port=14
```

Chapter 9

MAC Address Table Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the MAC address table.

ADD SWITCH FDB|FILTER

Syntax

```
add switch fdb|filter
destaddress|macaddress=macaddress port=port
vlan=name|vid
```

Note
The FDB and FILTER keywords are equivalent.

Parameters

destaddress 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) to which the MAC address is to be assigned. You can specify only one port if you are adding a unicast address. You can specify more than one port if you are entering a multicast address.
vlan	Specifies the name or the VID of the VLAN to which the node designated by the MAC address is a member.

Description

This command adds 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, the address must be assigned to the port when the multicast application is located and to the ports where the host nodes are connected. Assigning the address only to the port where the multicast application is located will result in the failure of the multicast packets to be properly forwarded to the host nodes.

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=00A0D2181A11 port=7
vlan=default_vlan
```

The following command adds the multicast MAC address 01:00:51:00:00 10 to ports 1 to 5. The ports belong to the Engineering VLAN:

```
add switch fdb macaddress=010051000010 port=1-5
vlan=Engineering
```

DELETE SWITCH FDB

Syntax

```
delete switch fdb macaddress=macaddress
vlan=name|vid
```

Parameters

macaddress — Specifies the dynamic or static unicast or multicast MAC address to delete from the MAC address table. The address can be entered in either of the following formats:

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

vlan — Specifies the VLAN containing the port(s) where the address was learned or assigned. The VLAN can be specified by name or VID.

Description

This command deletes dynamic and static unicast and multicast addresses from the switch's MAC address table.

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=00A0D2181A11 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=00a0c1112244
vlan=sales
```

RESET SWITCH FDB

Syntax

```
reset switch fdb port=port
```

Parameters

port	Specifies the port whose dynamic MAC addresses you want to delete from the MAC address table. You can specify more than one port at a time.

Description

This command deletes the dynamic MAC addresses learned on a specified port. Once a port's dynamic MAC addresses have been deleted, the port begins to learn new addresses.

Examples

The following command deletes all dynamic MAC addresses learned on port 5:

```
reset switch fdb port=5
```

SET SWITCH AGINGTIMER|AGEINGTIMER

Syntax

```
set switch agingtimer|ageingtimer=value
```

Parameter

agingtimer
ageingtimer

Specifies the aging timer for the MAC address table. The value is in seconds. The range is 0 to 1048575 seconds. The default is 300 seconds (5 minutes). Entering the value 0 (zero) disables the aging timer. The parameters are equivalent.

Description

The switch uses the aging timer to delete inactive dynamic MAC addresses from the MAC address table. When the switch detects that no packets have been sent to or received from a particular MAC address in the table after the period specified by the aging time, the switch deletes the address. This prevents the table from becoming full of addresses of nodes that are no longer active.

The value 0 (zero) disables the aging timer. When disabled, no dynamic addresses are deleted from the table, even addresses that belong to inactive nodes.

Example

The following command sets the aging timer to 120 seconds (2 minutes):

```
set switch agingtimer=120
```

SHOW SWITCH AGINGTIMER|AGEINGTIMER

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.

Example

This command displays the current setting for the MAC address aging timer:

```
show switch agingtimer
```

SHOW SWITCH FDB

Syntax

```
show switch fdb [address=macaddress] [port=port]
[status=static|dynamic|multicast] [vlan=name]
```

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.

status Specifies the type of MAC addresses you want to view. Choices are static, dynamic, and multicast. If no status is stated, the command displays the static and dynamic unicast 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.

Note
You can specify more than one parameter at a time with this command.

Description

This command displays the MAC addresses learned or assigned to the ports on the switch.

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 status=static
```

The following command displays the static and dynamic multicast addresses:

```
show switch fdb status=multicast
```

The following command displays the port on which 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 status=static
```

Chapter 10
Port Trunking Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information and guidelines on port trunking.

ADD SWITCH TRUNK

Syntax

```
add switch trunk=name port=port
```

Parameters

trunk	Specifies the name of the port trunk to be modified.
port	Specifies the port to be added to the port trunk. You can add more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

Description

This command adds ports to an existing port trunk. To view the trunks on a switch, refer to SHOW SWITCH TRUNK on page 193. To initially create a port trunk, refer to CREATE SWITCH TRUNK on page 188.

⚠ **Caution**
Disconnect all data 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 should check to see that 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.

Example

The following command adds port 5 to a port trunk called load22:

```
add switch trunk=load22 port=5
```

CREATE SWITCH TRUNK

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. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).
select	The load distribution method. Options are:

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.

Description

This command creates a port trunk. To create the trunk, you specify the ports on the switch that will constitute the trunk and the load distribution method.

⚠ **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 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-S62 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.

Examples

The following command creates a 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 23. The command names the trunk "trunk4". No load distribution method is specified, so the default source and destination MAC addresses is used:

```
create switch trunk=trunk4 port=15,17,23
```

DELETE SWITCH TRUNK

Syntax

```
delete switch trunk=name port=port
```

Parameters

trunk	Specifies the name of the trunk to be modified.
port	Specifies the port to be removed from the existing port trunk. You can specify more than one port at a time.

Description

This command removes ports from a port trunk. To view the trunks on a switch, refer to SHOW SWITCH TRUNK on page 193. To completely remove a port trunk from a switch, see DESTROY SWITCH TRUNK on page 191.

⚠ **Caution**
Disconnect all 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.

Example

The following command removes port 9 from a port trunk called Dev_trunk:

```
delete switch trunk=Dev_trunk port=9
```

DESTROY SWITCH TRUNK

Syntax

```
destroy switch trunk=name
```

Parameter

trunk	Specifies the name of the trunk to be deleted.

Description

This command deletes a port trunk from a switch. Once 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 can create loops in your network topology. Data loops can result in broadcast storms and poor network performance.

Example

The following command deletes the trunk called load22 from the switch:

```
destroy switch trunk=load22
```

SET SWITCH TRUNK

Syntax

```
set switch trunk=name
select=[macsrc|macdest|macboth|ipsrc|ipdest|
ipboth]
```

Parameters

trunk Specifies the name of 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 changes the load distribution method of an existing port trunk. To view the trunks on a switch, refer to SHOW SWITCH TRUNK on page 193.

Example

The following command changes the load distribution method of a trunk named “Load11” to destination IP address:

```
set switch trunk=Load11 select=ipdest
```

SHOW SWITCH TRUNK

Syntax

```
show switch trunk
```

Parameters

None.

Description

This command displays the names, ports, and load distribution methods of the port trunks on the switch.

Example

The following command displays port trunking information:

```
show switch trunk
```

Chapter 11
Networking Stack Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information and guidelines on networking stack.

DELETE IP ARP

Syntax

```
delete ip arp [ipaddress|all]
```

Parameter

ipaddress	Specifies the IP address of the ARP entry you want to delete from the ARP table.
all	Specifies the deletion of all non-system ARP entries in the table.

Description

This command deletes specific or all ARP entries from the ARP table.

Example

The following command deletes the ARP entry with the IP address of 192.168.1.1:

```
delete ip arp 192.168.1.1
```

DELETE TCP

Syntax

```
delete tcp indexnumber
```

Parameter

indexnumber	Specifies the internal socket ID number assigned to the connection. Enter the index number of the TCP connection you want to delete. The range is 0 to 65535 with a default of 0. To display the index number, refer to SHOW TCP on page 201.

Description

This command deletes a TCP connection.

Example

The following command deletes TCP connection number 12:

```
delete tcp 12
```

RESET IP ARP

Syntax

```
reset ip arp
```

Parameter

None

Description

This command deletes all of the temporary entries in the ARP table.

Example

The following command deletes all non-system entries in the ARP table:

```
reset ip arp
```

SET IP ARP

Syntax

```
set ip arp [timeout=integer]
```

Parameter

timeout	The range is 1 to 260000 seconds. The default setting is 400 seconds.

Description

This command prevents the table from becoming full with inactive entries. It allows you to set the timer for removing temporary entries in the ARP table. Inactive temporary entries in the ARP table are timed out according to the ARP cache timeout value which is set with the timeout option.

Example

The following command sets the timer to 600 seconds:

```
set ip arp timeout=600
```

SHOW IP ARP

Syntax

```
show ip arp
```

Parameters

None

Description

This command displays the IP addresses in the ARP table. It includes the following fields:

Interface
The network interface of a table entry. The switch has two network interfaces. The "loopback" designation represents the interface used by the switch for internal diagnostics. The "eth0" designation represents the Ethernet network interface.

IP Address and
MAC Address
The IP addresses and their corresponding MAC addresses.

Type
The type of ARP entry. An entry can be permanent, meaning it can never be deleted from the table, or temporary. Only the "loopback" entry is permanent. All "eth0" entries are temporary.

Example

The following command displays the ARP table.

```
show ip arp
```

SHOW IP ROUTE

Syntax

```
show ip route
```

Parameter

None

Description

This command displays the IP route table. It includes the following fields:

Destination
The IP address of a destination network, subnetwork, or end node.

Mask
A filter used to designate the active part of the destination IP address. A binary 1 in the mask indicates an active bit in the address while a binary 0 indicates that the corresponding bit in the address is not.

Next Hop
The IP address of the next intermediary device to reaching the destination network, subnetwork, or end node.

Interface
The interface on the switch where the next hop is located. The switch has two interfaces. The interface "loopback" is for internal diagnostics only. The other interface is "eth0."

Example

The following command displays the IP route table:

```
show ip route
```

SHOW TCP

Syntax

```
show tcp
```

Parameter

None

Description

This command displays the TCP connections and the TCP global information which is MIB variables defined in TCP group. It includes the following fields:

RTO min (ms) and RTO max (min)
Retransmit time algorithm parameters.

Max connections
The maximum number of TCP connections allowed.

Active Opens
The number of active TCP opens. Active opens initiate connections.

Passive Opens
The number of TCP passive opens. Passive opens are issued to wait for a connection from another host.

Attempt Fails
The number of failed connection attempts.

Established Resets
The number of connections established but have not been reset.

Current Established
The number of current connections.

In Segs
The number of segments received.

In Segs Error
The number of segments received with an error.

Out Segs
The number of segments transmitted.

Out Segs Retran
The number of segments retransmitted.

Out Segs with RST

The number of segments transmitted with the RST bit set.

Total Number of TCP Listening sockets

The number of active listening sockets. There can be a maximum of three listening sockets. One is for the Telnet server, another for SSH, and the last for the web browser server. If a server is disabled, its listening socket does not appear in the table.

Total Number of TCP connections

The number of active Telnet, SSH, and web browser connections to the switch.

Index

The internal socket ID number assigned to the connection.

Local Address

The IP address of the switch, followed by the TCP port number used by the switch for the connection. The two values are divided by a colon, as illustrated in Figure 1. The port number indicates the type of TCP connection. A port number of 23 indicates a Telnet connection, 22 an SSH connection, and 80 or 443 a web browser HTTP or HTTPS connection, respectively.

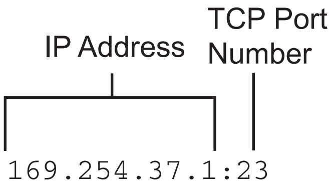


Figure 1 IP Address and TCP Port Number

Foreign Address

The IP address of the management workstation that initiated the connection, followed by the station's TCP port number.

State

The state of the TCP connection. A state of ESTABLISHED signals a successful TCP connection between the switch and the management workstation. For definitions of all the TCP states, refer to RFC-793.

The entries for the listening sockets for the Telnet, SSH, and web browser servers are identified in the table with a TCP state of LISTEN. If you disable a server on the switch, its corresponding LISTEN entry is removed from the table. Disabling all the servers leaves the table empty. (The SSH server is disabled by default on the switch.)

Example

The following command displays the TCP connections and the TCP global information:

```
show tcp
```

Chapter 12

LACP Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information and guidelines on LACP.

ADD LACP PORT

Syntax

```
add lacp port=port aggregator=name|adminkey=key
priority=priority
```

Parameters

port	Specifies the port to be added to the aggregator. You can add more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).
aggregator	Specifies the name of the aggregator. The name is case-sensitive.
adminkey	Specifies the adminkey of the aggregator. This is a hexadecimal number in the range 0x1 to 0xffff.
priority	Specifies the priority level of the port. This is a hexadecimal number in the range 0x1 to 0xffff. The lower the number, the higher the priority. The default is the port number in hexadecimal. For instance, the default priority level for port 10 is 0x000A.

Description

This command adds ports to an existing aggregator. You can set a port's priority value when you add it to an aggregator. You can identify the aggregator by its name or adminkey number. To create an aggregator, refer to CREATE LACP AGGREGATOR on page 207.

⚠ **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.

Note
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.

Example

The following command adds ports 8 and 22 to an aggregator named “agg_1”:

```
add lacp port=8,22 aggregator=agg_1
```

The following command adds port 6 to an aggregator with an adminkey number of 1A and assigns the port a priority of 0x10:

```
add lacp port=6 adminkey=0x1a priority=0x10
```

CREATE LACP AGGREGATOR

Syntax

```
create lacp aggregator=name adminkey=key port=port
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|
ipboth]
```

Parameters

aggregator — Specifies the name of the new aggregator. The name can be up to 20 alphanumeric characters. No spaces or special characters are allowed.

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. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

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.

⚠ **Caution**
Do not connect the cables to the ports of the aggregator on the switch until after you have configured the aggregator with the management software and enabled LACP. Connecting the cables before configuring the software and activating the protocol will create a loop in your network topology. Data loops can result in broadcast storms and poor network performance.

Note
Before creating an aggregator, 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.

Examples

The following command creates an LACP aggregator named “agg_1” of ports 1 through 4 and an adminkey of 4. The load distribution method is source MAC address:

```
create lacp aggregator=agg_1 adminkey=0x4 port=1-4
distribution=macsrc
```

The following command creates an LACP aggregator named “lacp_trunk1” of ports 10, 12, and 15 to 18. The adminkey number is 0x7A. No load distribution method is specified; the source and destination MAC addresses load distributed method is used by default:

```
create lacp aggregator=lacp_trunk1 adminkey=0x7A
port=10,12,15-18
```

DELETE LACP PORT

Syntax

```
delete lacp port=port [aggregator=name]
```

Parameters

port — Specifies the port to delete from an aggregator. You can delete more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

aggregator — Specifies the name of the aggregator. The name is case-sensitive. This parameter is optional.

Description

This command removes a port from an aggregator. You do not have to include the name of the aggregator in the command. If the port is not a member of an aggregator, this error message is displayed:

```
ERROR CODE = CLI_AGGREGATOR_KEY_DOES_NOT_EXIST
```

To completely remove an aggregator, see DESTROY LACP AGGREGATOR on page 210.

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.

Example

The following command removes port 9 from its current aggregator assignment:

```
delete lacp port=9
```

DESTROY LACP AGGREGATOR

Syntax

```
destroy lacp aggregator=name|adminkey=key
```

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.

⚠ **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
```

DISABLE LACP

Syntax

```
disable lacp
```

Parameters

None.

Description

This command disables LACP on the switch. The default is disabled. This command is equivalent to SET LACP STATE on page 217.

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 might occur, resulting in a broadcast storm and poor network performance.

Example

The following command disables LACP on the switch:

```
disable lacp
```

ENABLE LACP

Syntax

```
enable lacp
```

Parameters

None.

Description

This command enables LACP. The default is disabled. This command is equivalent to SET LACP STATE on page 217.

Example

The following command enables LACP:

```
enable lacp
```

SET LACP AGGREGATOR

Syntax

```
set lacp aggregator=name
[distribution=macsrc|macdest|macboth|ipsrc|ipdest|
ipboth] [adminkey=key]
```

Parameters

aggregator Specifies the name of the aggregator. The name is case-sensitive.

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.

adminkey Specifies a new adminkey number for the aggregator. This is a hexadecimal number between 0x1 and 0xffff.

Description

This command is used to modify an LACP aggregator's load distribution method or adminkey.

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 adminkey to 0x22 for the LACP aggregator named "server11_trunk":

```
set lacp aggregator=server11_trunk adminkey=0x22
```

SET LACP PORT

Syntax

```
set lacp port=port aggregator=name|adminkey=key
priority=priority
```

Parameters

port — Specifies the port to modify. You can modify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).

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 in the range 0x1 to 0xffff.

priority — Specifies the priority level of the port. This is a hexadecimal number in the range 0x1 to 0xffff. The lower the number, the higher the priority. The default is the port number in hexadecimal. For instance, the default priority level for port 10 is 0x000A.

Description

This command is used to assign a port to an aggregator or, if it is already assigned to one, change its assignment. You can specify the aggregator by its name or adminkey. This function can also be performed using ADD LACP PORT on page 205.

This command is also used to change a port's priority value.

To remove a port from an aggregator without assigning it to another aggregator, refer to DELETE LACP PORT on page 209.

⚠ **Caution**
If you will be adding or removing ports from the aggregator, you should disconnect all network cables from the ports of the aggregator on the switch before performing the procedure. Adding or removing ports without first disconnecting the cables can result in loops in your network topology, which can result in broadcast storms and poor network performance.

Note
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.

Examples

The following command adds ports 2 and 5 to an aggregator named "switch_trunk":

```
set lacp port=2,5 aggregator=switch_trunk
```

The following command adds ports 8 and 9 to an aggregator with the adminkey of 0x11:

```
set lacp port=8-9 adminkey=0x11
```

The following command changes the priority of port 6 to 0x2B:

```
set lacp port=6 priority=0x2b
```

SET LACP PRIORITY

Syntax

```
set lacp priority=priority
```

Parameters

priority	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 priority=0x8000
```

SET LACP STATE

Syntax

```
set lacp state=enable|disable
```

Parameters

state	Specifies the state of LACP on the switch. The options are:
	enable — Enables LACP. This option performs the same function as ENABLE LACP on page 212.
	disable — Disables LACP. This is the default. This option performs the same function as DISABLE LACP on page 211.

Description

This command enables or disables LACP on the switch.

⚠ **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 might occur, resulting in a broadcast storm and poor network performance.

Example

The following command enables LACP on the system:

```
set lacp state=enable
```

SHOW LACP

Syntax

```
show lacp [port=port|all] [aggregator=name]
[machine=port|all]
```

Parameter

port	Specifies the port(s) to display. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-20), or both (for example, 1,14-16).
aggregator	Specifies the name of the aggregator. The name is case-sensitive.
machine	Specifies the LACP machine state for a port or ports on the system.

Description

This command displays the configuration and/or machine states of the ports, and/or the aggregators.

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
```

Chapter 13
Port Mirroring Commands

This chapter contains the following commands:

- ❑ SET SWITCH MIRROR on page 220
- ❑ SET SWITCH PORT MIRROR on page 221
- ❑ SHOW SWITCH MIRROR on page 222

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information and guidelines on port mirroring.

SET SWITCH MIRROR

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 will be copied. You can specify only one port as the destination port. Specifying “0” (zero) disables port mirroring.

Description

This command enables mirroring and specifies the destination port, or disables mirroring. To select the source ports, refer to SET SWITCH PORT MIRROR on page 221.

Example

The following command enables mirroring and makes port 11 the destination port:

```
set switch mirror=11
```

The following command disables port mirroring:

```
set switch mirror=0
```

SET SWITCH PORT MIRROR

Syntax

```
set switch port=port mirror=none|rx|tx|both
```

Parameters

port	Specifies the source ports of a port mirror. You can specify more than one port. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).
mirror	Specifies which traffic on the source ports is 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 220.

Example

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
```

SHOW SWITCH MIRROR

Syntax

```
show switch mirror
```

Parameters

None.

Description

This command displays the source and destination ports of a port mirror on the switch.

Example

The following command displays the ports of a port mirror:

```
show switch mirror
```

Chapter 14
Statistics Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on statistics.

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 at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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 COUNTER

Syntax

```
show switch counter
```

Parameters

None.

Description

This command displays operating statistics, such as the number of packets received and transmitted, and the number of CRC errors, for the entire switch. For a list of and definitions for the statistics, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

Example

The following command displays the switch's operating statistics:

```
show switch counter
```

SHOW SWITCH PORT COUNTER

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 a list of and definitions for the statistics, refer to the *AT-S62 Management Software Menus Interface User's Guide.*

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 ports:

```
show switch port counter
```

Chapter 15

File System Commands

This chapter contains the following commands:

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the switch's file system.

COPY

Syntax

```
copy "filename1.ext" "filename2.ext"
```

Parameters

filename1.ext
Specifies the name of the file to be copied. If the name contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

filename2.ext
Specifies the name of the copy. If the name contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

Description

This command creates a copy of an existing file. The new filename must be a valid filename from 1 to 16 alphanumeric characters. The name of the copy must be unique from all other files in the file system.

ext is the three-letter file extension, and can be any of the following file types: ".cer", ".cfg", ".key" and ".csr". You must give the copy the same extension as the original file.

Note
You cannot copy files with a ".ukf" extension.

Example

The following command creates a copy of the configuration file "admin.cfg" and names the copy "admin2.cfg":

```
copy admin.cfg admin2.cfg
```

The following command creates a copy of the configuration file "switch 12.cfg" and names the copy "backup.cfg":

```
copy "switch 12.cfg" backup.cfg
```

CREATE CONFIG

Syntax

```
create config="filename.cfg"
```

Parameter

config — Specifies the name of a new configuration file. If the filename contains spaces, it must be enclosed in double quotes. Otherwise, the quotes are optional.

Description

This command creates a new configuration file containing the commands required to recreate the current configuration of the switch.

The CONFIG parameter specifies the name of the configuration file to create. 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 and 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 assign the new configuration file as the active boot configuration file, refer to SET CONFIG on page 232.

Example

The following command creates the new configuration file Switch12.cfg. The file will contain all of the commands necessary to recreate the switch's current configuration:

```
create config=Switch12.cfg
```

DELETE FILE

Syntax

```
delete file="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. You cannot use wildcards.

Description

This command deletes a file from the file system. To list the files in the file system, refer to SHOW FILE on page 234. When deleting a file, note the following:

- ❑ Deleting the configuration file that is acting as the active boot configuration file will cause 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 232.
- ❑ To delete a certificate, you must first remove the certificate from the certificate database using DELETE PKI CERTIFICATE on page 523.
- ❑ Files with a ".ukf" extension cannot be deleted with this command. These files are encryption key pairs. To delete an encryption key, refer to DESTROY ENCO KEY on page 512.

Example

The following command deletes the configuration file named Switch 12.cfg:

```
delete file="Switch 12.cfg"
```

The following command deletes the certificate enrollment request SW55a.csr:

```
delete file=SW55a.csr
```

RENAME

Syntax

```
rename "filename1.ext" "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.
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.

Description

This command renames a file. The source and destination file extensions must be the same.

Note
You cannot rename files with a ".ukf" extension.

Example

The following command renames the file "Switch12.cfg" to "Sw 44a.cfg":

```
rename Switch12.cfg "Sw 44a.cfg"
```

SET CONFIG

Syntax

```
set config="filename.cfg"
```

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, it must be enclosed in double quotes.

Description

This command sets the active configuration file for a switch. The switch uses the active configuration file to configure its parameter settings when it is rebooted or power cycled.

To view the name of the current active configuration file, see SHOW CONFIG on page 64.

You can specify a configuration file that already exists in the switch's file system, or one that does not. To view the configuration files already in a switch's file system, see SHOW FILE on page 234. Configuration files have a ".cfg" extension.

Note
The active boot configuration file is updated when you use the SAVE CONFIGURATION command.

Selecting a new active boot configuration file does not change the current configuration of the switch. If you want the switch to reconfigure itself according to the configuration in the newly assigned active boot configuration file, reset or power cycle the unit.

You do not need to use the SAVE CONFIGURATION command when you change the designated active configuration file. The change is saved to permanent memory automatically.

If you specify a nonexistent configuration file, the switch creates the file after you use the SAVE CONFIGURATION command.

Example

The following command sets the active boot configuration file to switch22.cfg:

```
set config=switch22.cfg
```

The switch uses the switch22.cfg configuration file to configure its settings the next time the unit is reset.

SHOW FILE

Syntax

```
show file=”filename”
```

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.

Description

This command displays a list of 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 display the contents of a configuration file.

Examples

This command displays all the files in the switch’s file system:

```
show file=*.*
```

This command displays all the configuration files on the switch:

```
show file=*.cfg
```

This command displays the contents of the configuration file sw12.cfg:

```
show file=sw12.cfg
```

Chapter 16
File Download and Upload Commands

This chapter contains the following commands:

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on downloading and uploading software images and configuration files.

LOAD METHOD=LOCAL

Syntax

```
load method=local destfile=appblock
srcfile|file=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-S62 image file.
srcfile *or* file	Specifies the filename of the AT-S62 image file in the file system that you want to download into the application block. If the filename contains a space, enclose the name in double quotes. These parameters are equivalent.

Description

A local download is used to download an AT-S62 image file already stored in the switch’s file system to the application block, which is the section of flash memory reserved for the active AT-S62 running image. This function makes the AT-S62 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-S62 image file into the file system of a switch and you now want to make that image file the switch’s active image file.

When performing a local download, note the following:

- ❑ The AT-S62 manage image that you want to be the new running image for the switch must already be stored in the switch’s file system.
- ❑ The command must include the DESTFILE parameter with the APPBLOCK option.
- ❑ Use the SRCFILE or FILE parameter to specify the name of the AT-S62 image file as it is stored in the switch’s file system.
- ❑ The current configuration of a switch is retained when a new AT-S62 software image copied to the application block.

❑ Once you have downloaded an image file from the file system to the application block, you can delete the image file from the file system to free up space for other files.

Example

This command downloads an AT-S62 image file already stored in the switch’s file system into the application block, which is 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 “ats62v1 3 0.img”:

```
load method=local destfile=appblock
srcfile=”ats62v1 3 0.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.

⚠ **Caution**
After downloading an AT-S62 image file into the application block from its file system, the switch resets itself and initializes its management 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.

LOAD METHOD=TFTP

Syntax

```
load method=tftp destfile=appblock|filename
server=ipaddress srcfile|file=filename
```

Parameters

method — Specifies a TFTP download.

destfile — Specifies the destination filename for the file. 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 any files already stored in the file system. The command will not overwrite a preexisting file with the same name.

The APPBLOCK option specifies the application block of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S62 image file. The APPBLOCK option is used to download a new AT-S62 image file from a TFTP server to the application block of the switch so that it functions as the new active image file on the switch.

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.

Description

An TFTP download uses the TFTP client software on the switch to download files onto the unit from a TFTP server on your network. For example, you might use the command to update a switch's AT-S62 image file, or to download a different boot configuration file or a SSL public key certificate.

Note
In previous versions of the AT-S62 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 248

The DESTFILE parameter specifies a name for the file as it will be stored in the file system on the switch. Enclose the name in double quotes if it contains a space. 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 1.

Table 1 File Name Extensions

Extension	File Type
.cfg	AT-S62 configuration file
.cer	Public key certificate
.csr	Public key certificate enrollment request
.key	Encryption key file
.img	AT-S62 management software image

The APPBLOCK option of the DESTFILE parameter refers to the switch's application block, which is the portion of flash memory reserved for the active AT-S62 image. This option downloads a new version of the AT-S62 image file into the application block, making it the active image file on the switch.

Note
The APPBLOCK option should only be used when downloading a new AT-S62 image file, and not with any other file type.

The equivalent FILE and SCRFILE parameters specify the name of the file on the TFTP server to download onto the switch.

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 that contains TFTP server software and the file to be downloaded must be stored on the server.

❑ You should start the TFTP server software before you perform the download command.

❑ The switch where you are downloading the file must have an IP address and subnet mask, such as a master switch. For switches without an IP address, such as a slave switch, you can perform an Xmodem download from a local management session or, alternatively, a switch to switch upload using UPLOAD METHOD=REMOTESWITCH on page 248.

❑ If you are downloading a configuration file, the switch does not automatically designate it as its active boot configuration file. To designate a configuration file as the active boot file, refer to SET CONFIG on page 232.

❑ The AT-S62 software image can be downloaded only onto an AT-8500 Series switch.

❑ The current configuration of a switch is retained when a new AT-S62 software image is installed.

❑ The AT-S62 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.

❑ If you download a new AT-S62 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 into the application block so that its used by the switch as its active image file, refer to UPLOAD METHOD=LOCAL on page 246.

Note
Downloading an AT-S62 image file into a switch's file system rather than into the application block should be perform with care. The file will take up nearly all 2 megabytes of space in the file system, leaving little room for other files, such as configuration files and SSL certificates.

Examples

The following command downloads a new configuration file into the switch's file system using TFTP. The configuration file is stored as "sw 111.cfg" on the TFTP server and is given the name "sw56a.cfg" when 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"
```

The following command downloads an SSL certificate to the switch's file system. The name of the file on the TFTP server is "sw12_ssl.cer". The same name is used for the file in the switch's file system:

```
load method=tftp destfile=sw12_ssl.cer
server=149.44.44.44 srcfile=sw12_ssl.cer
```

The following command uses the APPBLOCK option of the DESTFILE parameter to download a new version of the AT-S62 software image directly to the switch's application block, making the file the active image file on the switch. The IP address of the TFTP server is 149.11.11.11 and the name of the image file on the server is "ats62v130.img":

```
load method=tftp destfile=appblock
server=149.11.11.11 srcfile=ats62v130.img
```

⚠ **Caution**

After downloading an AT-S62 image file and writing it to the application block portion of flash memory, the switch resets itself and initializes its management 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 downloads a new version of the AT-S62 image file from a TFTP server to the switch's file system, changing the name from "ats62v1_3_0.img" to "ats62.img":

```
load method=tftp destfile=ats62.img
server=149.11.11.11 srcfile=ats62v130.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 246.

LOAD METHOD=XMODEM

Syntax

```
load method=xmodem destfile=appblock|filename
```

Parameters

method Specifies an Xmodem download.

destfile Specifies the destination filename for the file. 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 any files already stored in the file system. The command will not overwrite a preexisting file with the same name.

The APPBLOCK option specifies the application block of the switch's flash memory. This is the area of memory reserved for the switch's active AT-S62 image file. The APPBLOCK option is used to download a new AT-S62 image file into the application block so that it functions as the new active image file on the switch.

Description

An XMODEM download uses the XMODEM utility to download files onto a switch from a terminal or computer with a terminal emulator program connected to the switch's RS232 Terminal Port. You might use the command to update a switch's AT-S62 image file, or to download a different boot configuration file or a SSL public key certificate.

Note
In previous versions of the AT-S62 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 248

The DESTFILE parameter specifies a name for the file. This is the name the file will be stored as in the file system on the switch. Enclose the name in double quotes if it contains a space. When specifying the new name of a downloaded file, you must be sure to give it the correct three-letter extension, depending on the file type. The extensions are shown in Table 1 on page 239.

The APPBLOCK option of the DESTFILE parameter refers to the switch's application block, which is the portion of flash memory reserved for the active AT-S62 image. This option downloads a new version of the AT-S62 image file into the application block, making it the active image file on the switch.

Note
The APPBLOCK option should only be used when downloading a new AT-S62 image file, and not with any other file type.

Before downloading a file onto a switch using Xmodem, note the following:

- ❑ An Xmodem download is possible only from a local management session on a switch.
- ❑ Xmodem can download a file only onto the switch where you started the local management session. It cannot download a file through enhanced stacking.
- ❑ The file to download must be stored on the computer or terminal connected to the RS232 Terminal Port on the switch.
- ❑ The transfer protocol can be Xmodem or 1K Xmodem.
- ❑ When downloading a new configuration file, the switch does not automatically designate the file as its active boot configuration file. To designate a configuration file as the active boot file, refer to SET CONFIG on page 232.
- ❑ The AT-S62 software image is supported only on AT-8500 Series switches.
- ❑ The current configuration of a switch is retained when a new AT-S62 software image is installed.
- ❑ The AT-S62 image file contains the bootloader for the switch. You cannot load the image file and bootloader separately.
- ❑ If you download a new AT-S62 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 236.

Note
Downloading an AT-S62 image file into a switch's file system rather than into the application block should be perform with care. The file will take up most of the 2 megabytes of space in the file system, leaving little room for other files, such as configuration files and SSL certificates.

Examples

The following command downloads a new configuration file onto the switch. The configuration file is given the name "switch12.cfg" in the switch's file system:

```
load method=xmodem destfile=switch12.cfg
```

The source file is not specified when downloading a file using Xmodem. Rather, after you enter the command, the management software displays a confirmation prompt followed by another prompt instructing you to begin the file transfer. To start the transfer, you use your terminal emulation program to specify the file on your workstation that you want to download.

The following 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
```

The following command uses the APPBLOCK option of the DESTFILE parameter to download a new version of the AT-S62 software image directly to the application block, making the file the active image file on the switch:

```
load method=xmodem destfile=appblock
```

Caution
After downloading an AT-S62 image file and writing it to the application block portion of flash memory, the switch resets itself 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 downloads a new version of the AT-S62 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 “ats62v1_3_0.img”. The image file is stored in the switch’s file system with this name:

```
load method=xmodem destfile=ats62v1_3_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 236.

UPLOAD METHOD=LOCAL

Syntax

```
upload method=local destfile=filename
srcfile|file=appblock
```

Parameters

method	Specifies a local upload.
destfile	Specifies a filename for the AT-S62 image file. If the name contains spaces, enclose the name in quotes.
srcfile *or* file	Specifies the application block (APPBLOCK), where the active AT-S62 image file is stored.

Description

This command copies the switch's active AT-S62 image file from the application block, where the active AT-S62 image is stored, into the switch's file system.

Note
It is unlikely you will ever need to perform this type of upload.

Note
Uploading the active AT-S62 image file into a switch's file system should be perform with care. The file will take up most of the 2 megabytes of space in the file system, leaving little room for other files, such as configuration files and SSL certificates.

The DESTFILE parameter specifies a name for the file. This is the name given to the AT-S62 image file when uploaded from the application block to the file system. The name should include the suffix ".img".

The equivalent SRCFILE and FILE parameters specify APPBLOCK, for application block.

The optional VERBOSE parameter is only used with the REMOTESWITCH upload. It is used to monitor the progress of the upload process.

Example

The following command uploads the active AT-S62 image from the switch’s application block to the file system and assigns it the name “sw12 s62 image.img”:

```
upload method=local destfile=”sw12 s62 image.img”
src=appblock
```

UPLOAD METHOD=REMOTESWITCH

Syntax

```
upload method=remoteswitch
srcfile|file=appblock|switchcfg|filename
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* — Specifies the name of a configuration file in the master switch's file system.
- appblock — Uploads the master switch's active AT-S62 image file.
- switchcfg — Uploads the master switch's active boot configuration file.

switchlist — Specifies the switches in an enhanced stack to which to upload a file or the AT-S62 image file from the master switch. (To view the switches in an enhanced stack, see SHOW REMOTELIST on page 35.) 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 a boot configuration file or an active AT-S62 file image from a master switch to other switches in an enhanced stack. This is refer to as a switch to switch upload.

This command offers a simply means for updating multiple switches in a stack. For instance, to update switches with a new version of the AT-S62 image file, you can update the master switch first and then use a switch to switch upload to update the other switches in the stack.

You can also have a master switch distribute a configuration file to the other switches. This is useful in situations where the switches will share a similar configuration because it can save you from having to configure the switches individually.

When performing a switch to switch upload, note the following:

- ❑ The command must be performed from a management session of a master switch.
- ❑ You can perform a switch to switch upload from a local, Telnet, or SSH management session.
- ❑ You must perform the SHOW REMOTELIST command before performing this command. The command displays the switch numbers and also allows the management software to determine which switches are in the enhanced stack. For instructions, refer to SHOW REMOTELIST on page 35.
- ❑ You can upload the master switch's active AT-S62 image file, its active configuration file, or another configuration file stored in its file system to other switches. You cannot upload any other type of file, such as an encryption key or SSL certificate.
- ❑ You do not specify a destination filename in a switch to switch upload. A configuration file retains its original name on the switches where it is uploaded.
- ❑ When uploading the master switch's active AT-S62 image file to other switches, the file is copied directly to the application block on the other switches, automatically making it the active image file. It is not copied to the file system. This results in a switch reset. Some network traffic may be lost while the switch reloads its operating software.
- ❑ Once the upload of a configuration file is complete, the switch that received the configuration file marks it as the its boot configuration file and automatically resets. Some network traffic may be lost while the switch reloads its operating software. After the reset is complete, the switch operates with the parameter settings contained in the uploaded configuration file.
- ❑ When uploading a configuration file, the command syntax gives you the choice of downloading the master switch's current boot configuration file or another configuration file in the switch's file

system. To select the switch's current configuration file, use the SWITCHCFG option of the SRCFILE or FILE parameter. To upload another configuration file, omit the SWITCHCFG option and instead specify the file's name.

- If you use the SWITCHCFG option to upload the switch's current boot configuration file, the following information in the file is not included in the transfer: IP address, subnet mask, gateway address, switch name, contact, location, and the master mode setting. However, the switch receiving the configuration file does not retain its current settings to these parameters. Rather, they are returned to their default values.

- If you choose to upload a configuration file from the master switch's file system by specifying its filename, the entire file without modifications is uploaded. This type of configuration file upload should be performed with care. If the master switch has a manually assigned IP address, the switch receiving the configuration file will end up with the same IP address as the master switch.

- A configuration file should only be uploaded onto a switch of the same model from which the configuration file originated (for example, AT-8524M to AT-8524M). Allied Telesyn does not recommend uploading a configuration file onto a switch of a different model (for example, AT-8524M to AT-8516F/SC). Undesired switch behavior may result.

- The optional VERBOSE parameter is used to monitor the status of an upload.

The equivalent SRCFILE and FILE parameters specify the name of the file that you want to upload from the switch. You have three options:

- SWITCHCFG - Uploads the master switch's active boot configuration file.

- *filename* - Uploads a configuration file from the master switch's file system. This differs from the SWITCHCFG parameter in that the latter uploads just the active boot configuration file, while this parameter allows you to upload any configuration file in the master switch's file system.

- APPBLOCK - Uploads the master switch's active AT-S62 image file.

The optional VERBOSE parameter is used to monitor the progress of the upload process.

Examples

The following command uploads the active AT-S62 image file on a master switch to switch 2 in an enhanced stack. (Switch numbers are displayed with SHOW REMOTELIST on page 35.)

```
upload method=remoteswitch srcfile=appblock
switchlist=2
```

The active AT-S62 image file on the master switch is indicated with the APPBLOCK option of the SRCFILE parameter.

⚠ **Caution**

After a switch receives the AT-S62 image file, it resets itself 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.

You can upload the AT-S62 image file from the master switch to more than one switch at a time. The following command uploads the active 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 switches 11 and 12:

```
upload method=remoteswitch srcfile=switchcfg
switchlist=11,12
```

Since the current configuration file was designated with the SWITCHCFG option rather than its filename, the following information in the file is not included in the upload: IP address, subnet mask, gateway address, switch name, contact, location, and the master mode setting. However, the switch receiving the configuration file does not retain its current settings to these parameters. Rather, they are returned to their default values.

⚠ **Caution**

After a switch receives the configuration file, it resets itself 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
```

After the switch receives the file, it marks the file as its active boot configuration file and automatically resets itself so that it starts running with the new settings.

Since the configuration file was designated by its filename, the entire file without modifications is uploaded. This type of configuration file upload should be performed with care. If the master switch has a manually assigned IP address, the switch receiving the configuration file will end up with the same IP address as the master switch.

UPLOAD METHOD=TFTP

Syntax

```
upload method=tftp destfile=filename
server=ipaddress
srcfile|file=switchcfg|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.
appblock	Uploads the switch's active AT-S62 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. The command also allows you to upload the switch's active AT-S62 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 switch from where you are uploading the file must have an IP address and subnet mask, such as a master switch of an enhanced stack. To upload a file from a switch that does not have an IP address, such as a slave switch, you can perform an Xmodem upload from a local management session.

The DESTFILE parameter specifies a name for the file. This is the name that the file will be stored as on the TFTP server. When you name an uploaded file, you should give it the three-letter extension that corresponds to its file type. The extensions are listed in Table 1 on page 239.

The SERVER parameter specifies the IP address of the network node containing 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.
- ❑ APPBLOCK - Uploads the switch's active AT-S62 image file to the TFTP server.

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" 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 the switch's active AT-S62 image file to a TFTP server with an IP addresses 149.55.55.55:

```
upload method=tftp destfile="ats62 sw12.img"
server=149.55.55.55 srcfile=appblock
```

Note
It is unlikely you will ever have cause to upload an active image file from a switch to a TFTP server. If you are considering the upload so as to update the image file on another switch, you can simplify the process by instead performing a switch to switch upload using UPLOAD METHOD=REMOTESWITCH on page 248.

UPLOAD METHOD=XMODEM

Syntax

```
upload method=xmodem
srcfile|file=switchcfg|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 in the switch’s file system.
appblock	Uploads the switch’s active AT-S62 image file.

Description

An XMODEM upload uses the Xmodem utility to upload a file from the switch 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. The command also allows you to upload the switch’s active AT-S62 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 that you want 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. 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 switch's file system.
- ❑ APPBLOCK - Uploads the switch's active AT-S62 image file.

Examples

The following command uses Xmodem to upload a configuration file called "sw22 boot.cfg" from the switch's file system to the workstation where you are running the local management session:

```
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 you want to store the file on your workstation and its filename.

The following command uses Xmodem to upload 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 uploads the switch's active AT-S62 image file to the workstation:

```
upload method=xmodem srcfile=sw12_ssl_enroll.csr
```

Note
It is unlikely you will ever have cause to upload an active image file from a switch to your workstation. If you are considering the upload so as to update the image file on another switch, you can simplify the process by instead performing a switch to switch upload using UPLOAD METHOD=REMOTESWITCH on page 248.

Chapter 17

Event Log and Syslog Server Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command. For more information about the event log and syslog server definitions, refer to the *AT-S62 Management Software Menus Interface User’s Guide*.

ADD LOG OUTPUT

Syntax

```
add log output=id_number module=all|module
severity=all|severity
```

Parameters

output Specifies the ID number of a syslog server definition.

module Specifies the AT-S62 modules whose events are to be sent to the syslog server. The available options are:

- all Sends events from all modules.
- module Sends events from selected module(s). To specify more than one module, separate them with commas, for example, MAC,PACCESS. For a list of the modules, see Table 4 on page 279.

severity Specifies the severity of events to send to the syslog server. The options are:

- all Sends events of all severity levels.
- severity Sends events of a selected severity. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can specify more than one severity (for example, E,W). For a definition of the severity levels, see Table 5, "Event Log Severity Levels" on page 281.

Description

This command configures a syslog server definition.

There are two steps to creating a syslog server definition from the command line interface. The first is to create the definition using CREATE LOG OUTPUT on page 262. 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 to syslog server. This is accomplished with this command. You can customize the definition so that the switch sends all of its event messages to the server or limit it to just a selection of events from particular modules in the AT-S62 management software. An alternative method to configuring a definition is with SET LOG OUTPUT on page 275.

Note
The default configuration for a new syslog server definition specifies no event messages. The switch will not send events to the syslog server until you have customized the definition with this command or SET LOG OUTPUT on page 275.

The OUTPUT parameter specifies the ID number of the syslog server definition 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 283.

The MODULE parameter specifies the modules whose events you want the switch to send to the syslog server. The AT-S62 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 4 on page 279.

The SEVERITY parameter specifies the severity of the events to send to the server. For example, you might configure the switch to send only error events of all the modules. Or, you might configure a syslog server 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 5 on page 281.

Examples

The following command configures syslog server definition 5 to send all event messages of all severity levels:

```
add log output=5 module=all severity=all
```

The following command configures syslog server definition 3 to send only those event messages from the enhanced stacking module that have an error severity level:

```
add log output=3 module=estack severity=e
```

The following command configures syslog server definition 5 to send warning and error event messages from the spanning tree protocol and VLAN modules to the syslog server:

```
add log output=4 module=stp,vlan severity=e,w
```

CREATE LOG OUTPUT

Syntax

```
create log output=id_number destination=syslog
server=ipaddress
[facility=default|local1|local2|local3|local4|loc
al5|local6|local7] [syslogformat=extended|normal]
```

Parameters

output
: Specifies an ID number for the new syslog server definition. The range is 2 to 20. Each definition must be given a unique ID number.

destination
: Specifies the destination for the event 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 the syslog facility levels 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-S62 management software and its modules are shown in Table 2 on page 264. 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 3 on page 265.

syslogformat
: Specifies the format of the events. The possible options are:

extended
: Sends the severity, module, and description, date, time, and switch's IP address. This is the default.

normal
: Sends the severity, module, and description.

Description

This command creates a new syslog server definition. The switch uses the definition to send event messages to a syslog server on your network. You can create up to nineteen syslog server definitions.

After you create a new syslog server definition with this command, you must customize it by defining which event messages you want the switch to send to the server. You can customize a definition so that the switch sends all of its event messages to the syslog server or limit it to just a selection of events from particular modules in the AT-S62 management software. Customizing a definition is accomplished with ADD LOG OUTPUT on page 259 or SET LOG OUTPUT on page 275.

Note
The default configuration for a new syslog server definition specifies no event messages. The switch will not send events to the syslog server until you have customized the definition.

The OUTPUT parameter in this command specifies the ID number for the new syslog server 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 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-S62 management software and its modules are shown in Table 2.

Table 2 Applicable RFC 3164 Numerical Code and AT-S62 Module Mappings

Numerical Code	RFC 3164 Facility	AT-S62 Module
4	Security and authorization messages	Security modules: - PSEC - PACCESS - ENCO - PKI - SSH - SSL - MGMTACL - DOS Authentication modules: - SYSTEM - RADIUS - TACACS+
9	Clock daemon	Time- based modules: - TIME (system time and SNTP) - RTC
22	Local use 6	Physical interface and data link modules: - PCFG - PMIRR - PTRUNK - STP - VLAN
23	Local use 7	SYSTEM events related to major exceptions.
16	Local use 0	All other modules and events.

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 events from a switch the same numerical code using the LOCAL1 to LOCAL2 options. Each option represents a predefined RFC 3164 numerical code. The code mappings are listed in Table 3.

Table 3 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 a syslog server definition with an ID number 10. The IP address of the server is 149.65.10.999 and the messages are sent in normal format with a facility code of 22:

```
create log output=10 destination=syslog
server=149.65.10.99 facility=local6
syslogformat=normal
```

The following command creates output definition number 18. The messages are sent to the syslog server in extended format:

```
create log output=18 destination=syslog
server=149.65.10.101 syslogformat=extended
```

DESTROY LOG OUTPUT

Syntax

```
destroy log output=id_number
```

Parameters

output	Specifies the ID number of the syslog server definition to be deleted. The range is 2 to 20.

Description

This command deletes a syslog server definition. You can delete only one definition at a time. To disable the definition without deleting it, refer to DISABLE LOG OUTPUT on page 268.

Example

The following command deletes syslog server definition number 3:

```
destroy log output=3
```

DISABLE LOG

Syntax

```
disable log
```

Parameters

None.

Description

This command disables the event log module. When the log is disabled, the AT-S62 management software stops storing events in the log and sending events to the syslog servers. The default setting for the event log is enabled.

Note
The event log, even when disabled, logs all AT-S62 initialization events that occur when the switch is reset or power cycled. Any switch events that occur after AT-S62 initialization are recorded only if the event log is enabled.

Examples

The following command disables the event log on the switch:

```
disable log
```

DISABLE LOG OUTPUT

Syntax

```
disable log output[=id_number]
```

Parameters

output	Specifies the ID number of the syslog server definition to disable. The range is 2 to 20. You can specify only one ID number at a time. Omitting an ID number disables all syslog server definitions.

Description

This command disables the specified syslog server definition and stops the switch from sending any further system events to the defined server. To permanently remove a syslog server definition, see “DESTROY LOG OUTPUT” on page 266. To enable the syslog server definition again, see “ENABLE LOG OUTPUT” on page 270.

Examples

The following command disables (but does not delete) the syslog server definition with the ID number 7:

```
disable log output=7
```

The following command disables all syslog server definitions:

```
disable log output
```

ENABLE LOG

Syntax

```
enable log
```

Parameters

None.

Description

This command activates the event log. The switch begins to add events in the log and send events to defined syslog servers. The default setting for the event log is enabled.

Example

The following command activates the event log module on the switch:

```
enable log
```

ENABLE LOG OUTPUT

Syntax

```
enable log output[=id_number]
```

Parameters

output	Specifies the ID number of the syslog server definition you want to enable. The range is 2 to 20. You can specify only one ID number at a time. Omitting an ID number enables all syslog server definitions.

Description

This command enables the specified syslog server definition that was disabled using DISABLE LOG OUTPUT on page 268. When a syslog server definition is enabled, the switch immediately begins to send events to the server.

Examples

The following command enables syslog server definition 4:

```
enable log output=4
```

The following command activates all syslog server definitions:

```
enable log output
```

PURGE LOG

Syntax

```
purge log=temporary
```

Parameter

log	Specifies the location of the event log. There is only one option:	
	temporary	Specifies temporary memory. Deletes all events stored in the event log in temporary memory. The log has a storage capacity of 4,000 events.

Description

This command deletes all entries in the event log.

Example

The following command deletes all entries in the event log:

```
purge log=temporary
```

SAVE LOG

Syntax

```
save log=temporary filename=”filename.log” [full]
[module=module] [reverse] [severity=severity]
[overwrite]
```

Parameters

log — Specifies the location of the event log whose messages you want to save. There is only one option:

temporary — Specifies temporary memory. The log has a storage capacity of 4,000 events.

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-S62 module whose events are to be saved. For a list of modules, refer to Table 4 on page 279. Omitting this parameter saves messages from all modules.

reverse — Specifies the order in which the events are saved in the log. With this option, the events are saved newest to oldest. Without it, the events are saved oldest to newest.

severity — Specifies the severity of events to be saved to the log file. Choices are I for Informational, E for Error, W for Warning, and D for Debug. You can specify more than one severity (for example, E,W). For a definition of the severity levels, see Table 5, “Event Log Severity Levels” on page 281. Omitting this parameter saves messages of all severity levels.

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 file system.

Description

This command saves the current entries in the event log to a file in the switch’s file system. The parameters in the command allow you to specify which events you want saved in the file. Once the file is saved in the file system, you can either view the file or upload it to your management workstation.

Examples

The following command saves all of the events currently stored in the event log to a file called “switch 2.log”:

```
save log=temporary filename=”switch 2.log”
```

The following command saves just the error messages of the VLAN module in the full format to a file called “sw14.log”:

```
save log=temporary filename=sw14.log full
module=vlan severity=e
```

The following command saves the event messages generated by the spanning tree protocol and Quality of Service modules to a file called “stp_qos.log”. It saves only the informational and error messages in the full format and overwrites a file with an identical name already in the file system:

```
save log=temporary filename=stp_qos.log full
module=stp,qos severity=i,e overwrite
```

SET LOG FULLACTION

Syntax

```
set log fullaction temporary=halt|wrap
```

Parameter

temporary — Specifies the action of the event log when it reaches maximum capacity. The possible actions are:

halt	Stops storing new events.
wrap	Deletes the oldest entries when adding new ones. This is the default.

Description

This command controls the action of the event log when it reaches its maximum capacity of 4,000 events. You have two options. The first has the switch delete the oldest entries as it adds new entries to the log. The second has the switch stop adding new entries, so as to preserve the existing log contents.

The HALT option instructs the logs to stop storing new entries. If an event log has already reached maximum capacity, it immediately stops entering new entries.

The WRAP option instructs the logs to delete the oldest entries as new entries are added.

Note
A switch whose event log has reached maximum capacity continues to send events to syslog servers.

Example

The following command configures the event log to stop storing new events after it has stored its maximum number of entries:

```
set log fullaction temporary=halt
```

SET LOG OUTPUT

Syntax

```
set log output=id_number [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 the ID number of the syslog server definition to be modified. The range is 2 to 20.

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 definition.

facility — Specifies a new syslog facility level for the events.

- default — Adds a facility level based on the functional groupings defined in the RFC 3164 standard. The codes applicable to the AT-S62 management software and its modules are shown in Table 2 on page 264. 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 3 on page 265.

syslogformat Specifies the format of the event messages. The options are:

extended Sends the severity, module, and description, date, time, and switch's IP address for each event. This is the default.

normal Sends only the severity, module, and description.

module Specifies the AT-S62 modules whose events are to be sent to the syslog server. The available options are:

all Sends events from all modules.

module Sends events from selected module(s). You can select more than one module by separating them with commas, for example, MAC,PACCESS. For a list of modules, see Table 4 on page 279.

severity Specifies the severity of events to sent from the switch to the syslog server. Event severity is a predefined value assigned to an event by the switch, according to its impact on the switch's operation. The options are:

all Sends events of all severity levels.

severity Sends events of a particular severity level. 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 5 on page 281.

Description

This command modifies an existing syslog server definition created with CREATE LOG OUTPUT on page 262.

For information on the FACILITY parameter, refer to CREATE LOG OUTPUT on page 262. For information on the MODULE and SEVERITY parameters, refer to ADD LOG OUTPUT on page 259.

Examples

The following command changes the IP address for syslog server definition 3 to 198.45.12.1:

```
set log output=3 server=198.45.12.1
```

The following command changes the facility level and message format for syslog server 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
```

SHOW LOG

Syntax

```
show log=temporary [full] [module=module]
[reverse] [severity=severity]
```

Parameters

log
: Specifies the location of the event log. The only option is:

  temporary
  : Displays the events stored in temporary memory which can contain up to 4,000 events.

full
: Controls the format of the event 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-S62 module whose events you want displayed. You can specify more than one module by separating them with commas, for example, MAC,PACCESS. For a list of modules, refer to Table 4 on page 279. If you omit this parameter, the command displays the event messages from all the modules.

reverse
: Specifies the order in which the events are displayed. With this option, the events are displayed newest to oldest. Without it, the events are displayed oldest to newest.

severity
: Specifies the severity of the events to display. Event severity is a predefined value assigned to an event by the switch, according to its impact on the switch’s operation. 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 5, “Event Log Severity Levels” on page 281. If you omit this parameter, the command displays the informational, error, and warning messages.

Description

This command displays the entries stored in the switch's 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-S62 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 4 lists the modules and their abbreviations.

Table 4 AT-S62 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, DHCP, and BOOTP
LACP	Link Aggregation Control Protocol
MAC	MAC address table

Module Name	Description
MGMTACL	Management access control list
PACCESS	802.1x port-based access control
PCFG	Port configuration
POE	Power over Ethernet (AT-8524POE switch only)
PKI	Public Key Infrastructure
PMIRR	Port mirroring
PSEC	Port security (MAC address-based)
PTRUNK	Port trunking
QOS	Quality of Service
RADIUS	RADIUS authentication protocol
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

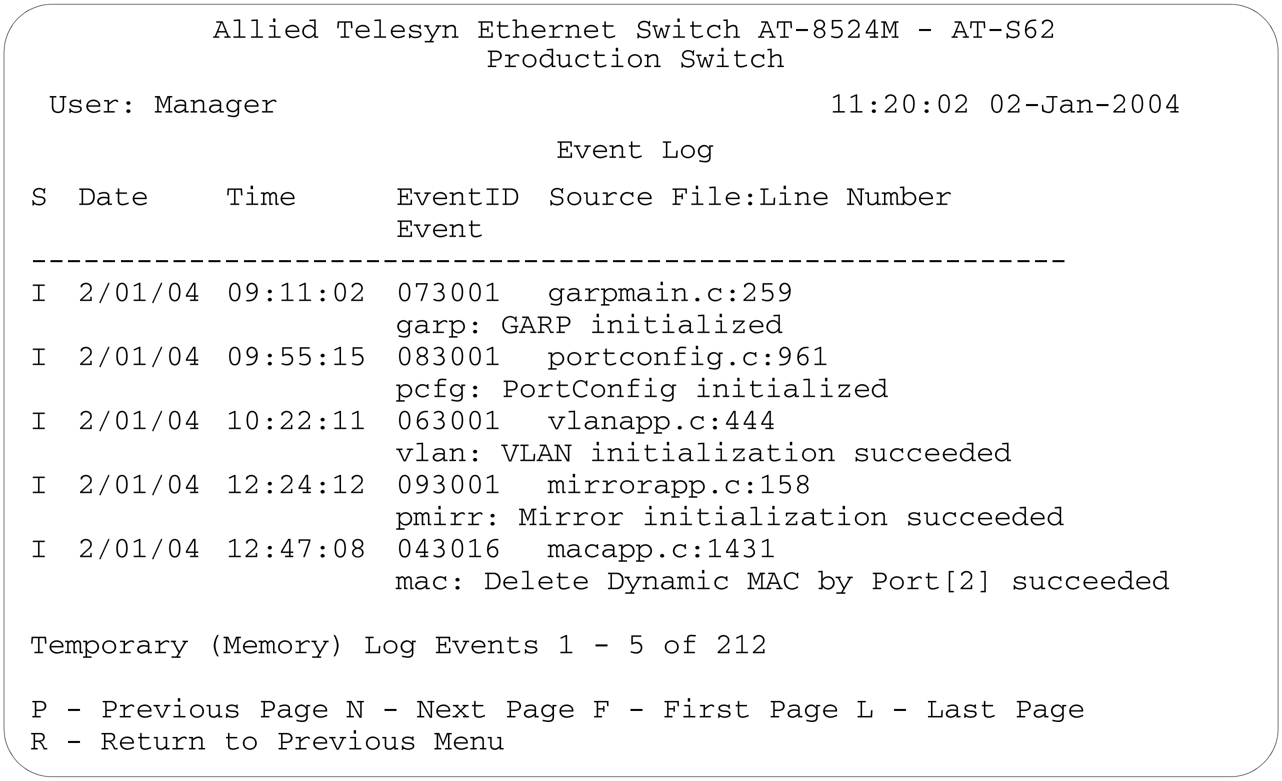
The log can display its entries in chronological order (oldest to newest), or reverse chronological order (newest to oldest). The default is chronological order. To reverse the order, use the REVERSE parameter.

The SEVERITY parameter displays entries of a particular severity. Table 5 defines the different severity levels. You can specify more than one severity level at a time. The default is error, warning, and informational messages.

Table 5 Event Log Severity Levels

Value	Severity Level	Description
ALL	-	Selects all severity levels.
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 1. The example uses the full display mode.



```
           Allied Telesyn Ethernet Switch AT-8524M - AT-S62
                           Production Switch

 User: Manager                                  11:20:02 02-Jan-2004
                              Event Log

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

Temporary (Memory) Log Events 1 - 5 of 212

P - Previous Page N - Next Page F - First Page L - Last Page
R - Return to Previous Menu
```

Figure 1 Event Log Example

The columns in the log are described below:

- ❑ S (Severity) - The event’s severity. Table 5 on page 281 defines the different severity levels.
- ❑ Date/Time - The date and time the event occurred.
- ❑ Event - The module within the AT-S62 software that generated the event followed by a brief description of the event. For a list of the AT-S62 modules, see Table 4 on page 279.
- ❑ Event ID - A unique number that identifies the event. (Displayed only in the Full display mode.)
- ❑ Filename and Line Number - The subsection of the AT-S62 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:

```
show log=temporary
```

The following command displays the events in the full display mode, which adds more information:

```
show log=temporary full
```

The following command displays only those entries from the file system and Quality of Service modules:

```
show log=temporary module=file,qos
```

The following command displays the error and warning entries from the VLAN module:

```
show log module=vlan severity=e,w
```

SHOW LOG OUTPUT

Syntax

```
show log output[=id_number] [full]
```

Parameters

output — Specifies the ID number of the event log or a syslog server definition. If an output ID number is not specified, all output definitions currently configured on the switch are displayed.

full — Displays the details of the syslog server definition. If not specified, only a summary is displayed.

Description

This command displays output definition details.

Entering the command without specifying an ID number of an output definition lists the event log and the syslog server definitions on the switch. Here is an example:

```
OutputID    Type          Status       Details
--------------------------------------------------
1           Temporary     Enabled      Wrap on Full
2           Syslog        Enabled      149.44.44.44
4           Syslog        Enabled      149.44.44.55
```

The event log has the ID number 1 and the Type of Temporary, referring to temporary memory, which is where the event log is stored.

Specifying "1" as the ID number along with the FULL option displays information about the event log. Here is an example:

```
Output ID .................... 1
Output Type .................. Temporary
Status ....................... Enabled
Log Full Action .............. Wrap on Full
Event Severity ............... All
Event Module ................. All
```

Entering the ID number of a syslog server definition along with the FULL option displays information about the definition. Here is an example:

```
Output ID .................... 2
Output Type .................. Syslog
Status ....................... Enabled
Server IP Address ............ 149.44.44.44
Message Format ............... Extended
Facility Level ............... DEFAULT
Event Severity ............... All
Event Module ................. All
```

Examples

The following command lists all the output definitions on the switch:

```
show log output
```

The following command displays information about the event log:

```
show log output=1 full
```

The following command displays complete information about syslog server definition 5:

```
show log output=5 full
```

SHOW LOG STATUS

Syntax

```
show log status
```

Parameter

None.

Description

This command displays information about the event log feature. Following is an example of what is displayed with this command:

```
Event Log Configuration:
Event Logging .................... Enabled
Number of Output Definitions ..... 4
```

The Event Logging field indicates whether the feature is enabled or disabled. When the log is enabled, the switch adds events to the log and sends events to syslog servers.

The Number of Output Definitions is a combination of the event log itself, which represents one output definition, and any syslog server definitions that currently exist. For instance, the number 4 for Number of Output Definitions in the above example indicates the existence of three syslog server definitions on the switch in addition to the event log.

Example

The following command displays event log status information:

```
show log status
```

Chapter 18
Classifier Commands

This chapter contains the following commands:

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on classifiers.

CREATE CLASSIFIER

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 be assigned a unique ID number. This parameter is required.

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

ethformat — Specifies an Ethernet frame type. Options are:

❑ ETHII-UNTAGGED - Ethernet II untagged packets

❑ ETHII-TAGGED - Ethernet II tagged packets

❑ 802.2-UNTAGGED - Ethernet 802.2 untagged packets

❑ 802.2-TAGGED - Ethernet 802.2 tagged packets 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 other Layer 2 protocols by entering the protocol number in either decimal or hexadecimal format. If you use 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, “IPDADDR=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 creates a classifier. A classifier defines a traffic flow. A traffic flow consists of packets that share one or more characteristics. A traffic flow can range from being very broad to being 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.

Classifiers are used with access control lists (ACL) and Quality of Service policies. The classifiers define the traffic flow to be affected by the ACL or QoS.

The ANY option of a parameter is used when you want to delete the current setting of a parameter without setting a new value. This leaves the parameter blank so that it applies to all packets.

Note
For definitions and restrictions on the classifier variables, refer to the *AT-S62 Management Software Menus Interface User's Guide.*

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 going to the destination IP address 149.44.44.44:

```
create classifier=7 description=”HTTPS flow”
ipdaddr=149.44.44.44 tcpdport=443
```

DESTROY CLASSIFIER

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 a classifier 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 297.

You cannot delete a classifier if it belongs to an ACL or QoS policy that has already been assigned to a port. You must first remove the port assignments from the ACL or policy before you can delete the classifier.

Example

This command deletes classifiers 2 and 4:

```
destroy classifier=2,4
```

PURGE CLASSIFIER

Syntax

```
purge classifier
```

Parameters

None.

Description

This command deletes all classifiers from the switch. You cannot delete a classifier if it belongs to an ACL or QoS policy that has already been assigned to a port. You must first remove the port assignments from the ACL or policy before you can delete the classifier.

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=integer]
[vlan=name|1..4094|any]
[protocol=ip|arp|rarp|number|any]
[iptos=integer|any] [ipdscp=integer|any]
[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 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 additional 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 modifies an existing classifier. The only setting of a classifier you cannot change is its ID number.

Specifying a new value for a variable that already has a value overwrites the current value with the new one. The ANY option removes a variable's value without assigning it a new value. A classifier must contain a least one variable with a value, besides the classifier ID and description.

You cannot modify a classifier if it belongs to an ACL or QoS policy that has already been assigned to a port. You must first remove the port assignments from the ACL or policy before you can modify the classifier.

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

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.

Examples

This command displays all of the classifiers:

```
show classifier
```

This command displays classifier ID 12:

```
show classifier=12
```

Chapter 19
ACL Commands

This chapter contains the following commands:

- ❑ CREATE ACL on page 299
- ❑ DESTROY ACL on page 301
- ❑ PURGE ACL on page 302
- ❑ SET ACL on page 303
- ❑ SHOW ACL on page 305

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on access control lists (ACL).

CREATE ACL

Syntax

```
create acl=integer [description="string"]
[action=deny|permit] classifierlist=integer
[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. The order in which you specify the classifiers is not important. An ACL must have at least one classifier.

portlist — Specifies the port where this ACL is to be assigned. You can assign an ACL to more than one port. When entering multiple ports, the ports can be listed individually (e.g., 2,5,7), as a range (e.g., 8-12) or both (e.g., 1-4,6,8).

Description

This command creates an ACL. An ACL is used to filter ingress packets on a port.

Example

The following command creates an ACL that discards the ingress traffic flow specified in classifier ID 18 and applies the ACL to port 4:

```
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 an ACL that permits the ingress traffic flow specified in classifier ID 18 and applies the ACL to ports 8 to 10:

```
create acl=24 description=”subnet flow deny”
action=permit classifierlist=18 portlist=8-10
```

DESTROY ACL

Syntax

```
destroy acl=integer
```

Parameters

acl	Specifies ID number of the ACL you want to delete. You can delete more than ACL at a time.

Description

This command deletes an ACL from the switch.

Example

The following command deletes ACL IDs 14 and 17:

```
destroy acl=14,17
```

PURGE ACL

Syntax

```
purge acl
```

Parameters

None.

Description

This command deletes all ACLs on the switch.

Example

This command deletes all ACLs on the switch:

```
purge acl
```

SET ACL

Syntax

```
set acl=integer [description=string]
[action=deny|permit] [classifierlist=integer]
[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 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.

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. 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 to be assigned this ACL. Any ports to which the ACL is assigned are overwritten. You can assign an ACL to more than one port. When entering multiple ports, the ports can be listed individually (e.g., 2,5,7), as a range (e.g., 8-12) or both (e.g., 1-4,6,8). 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 an ACL. You can use the command to change the description, action, classifiers, and ports of an ACL.

Example

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
```

SHOW ACL

Syntax

```
show acl[=integer]
```

Parameters

acl Specifies the ID of the ACL you want to view. You can specify more than one ACL at a time.

Description

This command displays the ACLs on the switch.

Example

This command displays all of the ACLs:

```
show acl
```

This command displays ACL ID 22:

```
show acl=22
```

Chapter 20

Quality of Service (QoS) Commands

This chapter contains the following commands:

- ❑ SHOW QOS POLICY on page 342
- ❑ SHOW QOS TRAFFICCLASS on page 343

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User’s Guide* for background information on Quality of Service.

ADD QOS FLOWGROUP

Syntax

```
add qos flowgroup=integer classifierlist=integers
```

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 an existing flow group. The classifiers must already exist. Any classifiers already assigned to the flow group are retained by the group. If you want to add classifiers while removing the those already assigned, refer to SET QOS FLOWGROUP on page 330.

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=integer trafficclasslist=integers
```

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 333.

Example

This command adds the traffic class 16 to policy 11:

```
add qos policy=11 trafficclasslist=16
```

ADD QOS TRAFFICCLASS

Syntax

```
add qos trafficclass=integer
flowgrouplist=integers
```

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 an existing traffic class. The flow groups must already exist. Any flow groups already assigned to the 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 337.

Examples

This command adds flow group 21 to traffic class 17:

```
add qos trafficclass=17 flowgrouplist=21
```

CREATE QOS FLOWGROUP

Syntax

```
create qos flowgroup=integer
[description="string"] [markvalue=integer|none]
[priority=integer|none]
[remarkpriority=yes|no|on|off|true|false]
[classifierlist=integers|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.

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 creates a new flow group.

> **Note**
> For examples of command sequences used to create entire QoS policies, refer to CREATE QOS POLICY on page 314.

Examples

This command creates a flow group with an ID of 10 and the description “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
```

CREATE QOS POLICY

Syntax

```
create qos policy=integer [description="string"]
[indscpoverwrite=integer|none]
[remarkindscp=all|none]
[trafficclasslist=integers|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 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.

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).

ingressport

Specifies the ingress ports to which the policy is to be assigned. Ports can be identified individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22).

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 creates a new QoS policy.

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

Creating a QoS policy involves a command sequence that creates 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 and limit the bandwidth to 5 Mbps. 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 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
```

CREATE QOS TRAFFICCLASS

Syntax

```
create qos trafficclass=integer
[description=”string”] [exceedaction=drop|remark]
[exceedremarkvalue=integer|none]
[markvalue=integer|none]
[maxbandwidth=integer|none]
[burstsize=integer|none] [priority=integer|none]
[remarkpriority=yes|no|on|off|true|false]
[flowgrouplist=integers|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. 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 in option 6. 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 in option 4, 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 option 3, Exceed Action. 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 option 6, Max Bandwidth. 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 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 four 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.
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 creates a new traffic class.

Note
For examples of command sequences used to create entire QoS policies, refer to CREATE QOS POLICY on page 314.

Examples

The following command creates a traffic class with an ID number of 25 and the description “Database flow”. The only parameter in the traffic class is the identification of the flow group, which is 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
```

DELETE QOS FLOWGROUP

Syntax

```
delete qos flowgroup=integer
classifierlist=integers
```

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 a flow group, it is unlikely you would ever use that option.)

Description

This command removes classifiers from a flow group.

Example

This command removes classifier 6 from flow group 22:

```
delete qos flowgroup=22 classifierlist=6
```

DELETE QOS POLICY

Syntax

```
delete qos policy=integer
trafficclasslist=integers
```

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=integer
flowgrouplist=integers
```

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

Syntax

```
destroy qos flowgroup=integer
```

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
```

DESTROY QOS POLICY

Syntax

```
destroy qos policy=integer
```

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
```

DESTROY QOS TRAFFICCLASS

Syntax

```
destroy qos trafficclass=integer
```

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.

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
```

SET QOS FLOWGROUP

Syntax

```
set qos flowgroup=integer [description=string]
[markvalue=integer|none] [priority=integer|NONE]
[remarkpriority=yes|no|on|off|true|false]
[classifierlist=integers|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.

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 308.

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 311.

> **Note**
> For examples of command sequences used to create entire QoS policies, refer to CREATE QOS POLICY on page 314.

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=integer [description=string]
[indscpoverwrite=integer|none]
[remarkindscp=[all|none]]
[trafficclasslist=integers|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.

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).

ingressport

Specifies the ingress ports to which the policy is to be assigned. Ports can be identified individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22). The NONE option removes the policy from all ingress ports to which it has been assigned. The ALL option adds it to all ports.

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 336, 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 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. The NONE option removes the policy from all egress ports to which it has been assigned. The ALL option adds it to all ports.

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 336, 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 314.

Note
For examples of command sequences used to create entire QoS policies, refer to CREATE QOS POLICY on page 314.

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=integer type=ingress|egress
policy=integer|none
```

Parameter

port
: Specifies the port to which the policy is to be assigned or removed. You can specify more than one port at a time if the port is an ingress port of the traffic flow. Ports can be identified individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22). You can specify only one port if the port is functioning as an egress port for the flow.

type
: Specifies whether the port is an ingress or egress port for the traffic flow of 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 currently assigned policy from a port.

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 QoS policy 12 to ingress ports 5 through 8:

```
set qos port=5-8 type=ingress policy=12
```

This command removes the currently assigned policy to egress ports 1 and 5:

```
set qos port=1,5 type=egress policy=none
```

SET QOS TRAFFICCLASS

Syntax

```
set qos trafficclass=integer
[description=”string”] [exceedaction=drop|remark]
[exceedremarkvalue=integer|none]
[markvalue=integer|none]
[maxbandwidth=integer|none]
[burstsize=integer|none] [priority=integer|none]
[remarkpriority=yes|no|on|off|true|false]
[flowgrouplist=integers|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 in option 6. 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 four 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 in option 4, Priority, if set to Yes. If set to No, which is the default, the packets retain their preexisting priority level when they leave the switch.

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 320. 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 314.

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

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.

Examples

This command displays all of the flow groups:

```
show qos flowgroup
```

This command displays flow group 12:

```
show qos flowgroup=12
```

SHOW QOS POLICY

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.

Examples

This command displays all of the policies:

```
show qos policy
```

This command displays policy 54:

```
show qos policy=54
```

SHOW QOS TRAFFICCLASS

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 (for example, 4,5,10).

Description

This command displays the traffic classes on a switch.

Examples

This command displays all of the traffic classes:

```
show qos trafficclass
```

This command displays traffic class 14:

```
show qos trafficclass=14
```

Chapter 21
Class of Service (CoS) Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on Quality of Service.

MAP QOS COSP

Syntax

```
map qos cosp=priority-number qid=queue-number
```

Parameters

cosp — Specifies the 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 assign more than one priority to an egress queue.

qid — Specifies the egress queue number. The egress queues are numbered 0 through 3, with queue 0 as the lowest priority and 3 as the highest. You can specify only one egress queue.

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 6 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Table 6 Default Mappings of IEEE 802.1p Priority Levels to Priority Queues

IEEE 802.1p Priority Level	Port Priority Queue
0	Q1
1	Q0
2	Q0
3	Q1
4	Q2
5	Q2
6	Q3
7	Q3

Note
This command is equivalent to SET QOS COSP on page 347.

Example

The following command maps priorities 4 and 5, to egress queue 3:

```
map qos cosp=4,5 qid=3
```

SET QOS COSP

Syntax

```
set qos cosp=priority-number qid=queue-number
```

Parameters

cosp	Specifies the 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 assign more than one priority to an egress queue.
qid	Specifies the egress queue number. The egress queues are numbered 0 through 3, with queue 0 as the lowest priority and 3 as the highest. You can specify only one egress queue.

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 6 on page 345 lists the default mappings between the eight CoS priority levels and the four egress queues of a switch port.

Note
This command is equivalent to MAP QOS COSP on page 345.

Example

The following command maps priorities 5 and 6, to egress queue 1:

```
set qos cosp=5,6 qid=1
```

SET QOS SCHEDULING

Syntax

```
set qos scheduling=strict|wrr weights=weights
```

Parameters

scheduling — Specifies the type of scheduling. The options are:

- strict — Strict priority. A 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. A port transmits a set number of packets from each queue in a round robin manner.

weights — Specifies the weight given to each of a port's four egress priority queues. You must specify the weights if scheduling will be weighted round robin. The range for each queue is 0 to 255 packets, and the default is 0. The weights are specified in the following order: Q0, Q1, Q2, Q3. For example, to give Q0 a weight of 1, Q1 a weight of 10, Q2 a weight of 20, and Q3 a weight of 30, you would enter this parameter as `weights=1,10,20,30`. The parameter must include all four queues.

Description

This command sets the QoS scheduling method and the weights for round robin scheduling. Scheduling and queue weights are set at the switch level. You cannot set this at a per-port basis.

Examples

The following command sets the scheduling to strict:

```
set qos scheduling=strict
```

The following command sets the scheduling to weighted round robin and gives egress priority queue Q0 a weight of 1, Q1 a weight of 5, Q2 a weight of 10, and Q3 a weight of 15:

```
set qos scheduling=wrr weights=1,5,10,15
```

SHOW QOS CONFIG

Syntax

```
show qos config
```

Parameters

None.

Description

Displays the QoS priority queues and scheduling.

Example

```
show qos config
```

Chapter 22

Power Over Ethernet Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on Power over Ethernet (PoE).

DISABLE POE PORT

Syntax

```
disable poe port=port
```

Parameters

port	Specifies a port. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command disables PoE on a port. The default setting for PoE on a port is enabled. The port continues to provide standard Ethernet connectivity even when PoE is disabled.

Examples

This command disables PoE on port 5 and 7:

```
disable poe port=5,7
```

ENABLE POE PORT

Syntax

```
enable poe port=port
```

Parameters

port	Specifies a port. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command activates PoE on a port. 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 specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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 PoE settings on a port.

The POEFUNCTION parameter 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.

The PRIORITY parameter is used to set a port's priority. The switch uses priorities to determine which ports are to receive PoE in the event the needs of the powered devices exceeds the available power resources of the switch. There are three levels: critical, high, and low. The default setting is low. Setting port priority on an AT-8524POE switch is not necessary since its power supply can deliver the maximum of 15.4 W to all 24 based ports simultaneously. For further information on PoE port priority, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

The POWERLIMIT parameter 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

The following command disables PoE on ports 4 and 5:

```
set poe port=4-5 poefunction=disable
```

This command sets the priority on port 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 THRESHOLD

Syntax

```
set poe threshold=value
```

Parameters

threshold	Specifies the threshold as a percentage of the total amount of PoE available. The range is 1 to 100.

Description

The PoE threshold sends an SNMP trap to your management workstation and enters an event in the event log when the total power requirements of the powered devices exceeds the specified percentage of the total maximum power available on the switch. At the default setting of 95%, the switch sends an SNMP trap when the PoE devices require more than 380 W, which is 95% of 400 W, the maximum available power on the AT-8524POE switch. The threshold is adjustable. Of course, for your management workstations to receive traps from the switch, you must configure SNMP on the switch by specifying the IP addresses of the workstations.

Examples

The following 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 specify more than one port at a time. You can specify the ports individually (e.g., 5,7,22), as a range (e.g., 18-23), or both (e.g., 1,5,14-22).

Description

Entering this command without specifying a port displays the following PoE information:

- ❑ Maximum available power - The total available power for PoE supplied by the switch. This value is 400 W for the AT-8524POE switch.
- ❑ Power threshold - A 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 380 W, which is 95% of 400 W, the maximum available power on the AT-8524POE 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 about port 4:

```
show poe config port=4
```

SHOW POE STATUS

Syntax

```
show poe status [port=port]
```

Parameter

port	Specifies a port. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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 400 W for the AT-8524POE 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 352 and DISABLE POE PORT on page 351.
- ❑ 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 353.
- ❑ Power Priority - The port priority. This can be Critical, High, or Low. To adjust this value, refer to SET POE PORT on page 353.
- ❑ 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 about port 4:

```
show poe status port=4
```

Chapter 23

IGMP Snooping Commands

This chapter contains the following commands:

- ❑ DISABLE IGMPSNOOPING on page 360
- ❑ ENABLE IGMPSNOOPING on page 361
- ❑ SET IP IGMP on page 362
- ❑ SHOW IGMPSNOOPING on page 364
- ❑ SHOW IP IGMP on page 365

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on IGMP Snooping.

DISABLE IGMPSNOOPING

Syntax

```
disable igmpsnooping
```

Parameters

None.

Description

This command deactivates IGMP snooping on the switch. This command performs the same function as the SNOOPINGSTATUS option in SET IP IGMP on page 362. The default setting for IGMP snooping is disabled.

Example

This command deactivates IGMP snooping:

```
disable igmpsnooping
```

ENABLE IGMPSNOOPING

Syntax

```
enable igmpsnooping
```

Parameters

None.

Description

This command activates IGMP snooping on the switch. This command performs the same function as the SNOOPINGSTATUS option in the command SET IP IGMP on page 362. The default setting for IGMP snooping is disabled.

Example

This command activates IGMP snooping:

```
enable igmpsnooping
```

SET IP IGMP

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. Possible settings 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 by the switch in determining inactive host nodes. An inactive host node is a node that has not sent an IGMP 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 256 addresses; the default is 64 addresses.

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 IGMP snooping parameters.

Example

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
```

SHOW IGMPSNOOPING

Syntax

```
show igmpsnooping
```

Parameters

None.

Description

This command displays the following IGMP parameters:

❑ IGMP snooping status

❑ Multicast host topology

❑ Host/router timeout interval

❑ Maximum multicast groups

❑ Multicast router ports

Note
To set the IGMP parameters, refer to SET IP IGMP on page 362.

Examples

The following command displays the current IGMP parameter settings:

```
show igmpsnooping
```

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 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 IGMP parameters:

- ❑ IGMP snooping status
- ❑ Multicast host topology
- ❑ Host/router timeout interval
- ❑ Maximum multicast groups
- ❑ Multicast router port(s)

This command, when performed without the HOSTLIST or ROUTERLIST parameter, performs the same function as SHOW IGMPSNOOPING on page 364. For instructions on how to set the IGMP parameters, refer to SET IP IGMP on page 362.

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
```

Chapter 24

Denial of Service (DoS) Defense Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on Denial of Service (DoS) attacks and the defense mechanisms employed by the management software.

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 (e.g., DSL router) that leads outside the network. You can specify only one port. This parameter is required for the Land defense. The default is the highest numbered existing port in the switch. For example, the default uplink port for an AT-8500 Series switch with no installed expansion modules would be Port 24.

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.

Here is an example. Let’s 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 21:

```
set dos ipaddress=149.22.22.1 subnet=0.0.0.255
uplinkport=21
```

SET DOS IPOPTION

Syntax

```
set dos ipoption port=port state=enable|disable
[mirrorport=port]
```

Parameters

port — Specifies the switch port on which 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.

mirrorport — Specifies a port where invalid traffic is copied. You can specify only one port.

Description

This command enables and disables the IP Options 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-S62 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:

- It sends a trap to the management workstations.
- The switch port discards all ingress packets containing IP options for a one minute period.

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.

Examples

The following command activates the IP Options defense on ports 5, 7, and 10:

```
set dos ipoption port=5,7,10 state=enable
```

SET DOS LAND

Syntax

```
set dos land port=port state=enable|disable
[mirrorport=port]
```

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.

mirrorport — Specifies a port where invalid traffic is copied. You can specify only one port.

Description

This command enables and disables the Land DoS defense. For an explanation of this attack and the AT-S62 defense mechanism, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

Examples

The following 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
[mirrorport=port]
```

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.

mirrorport Specifies a port where invalid traffic is copied. You can specify only one port.

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 workstations.
- ❑ The switch port discards the fragment and, for a one minute period, discards all ingress Ping packets on the port.

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, such as the processing of IGMP packets and spanning tree BPDUs. For this reason, Allied Telesyn recommends strictly limiting the use of this defense, activating it only on those ports where an attack is most likely to originate.

Examples

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 368. 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 workstations
- ❑ The port discards all ingress TCP-SYN packets for a one minute period.

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
[mirrorport=auto|port]
```

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.

mirrorport — Specifies a port where invalid traffic is copied. You can specify only one port.

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 workstations.
- ❑ The switch port discards the fragment with the invalid offset and, for a one minute period, discards all ingress IP fragments on the port.

Since the CPU examines only a sampling of the ingress IP traffic on a port, there is no guarantee that the switch will caught or prevent this type of attack.

⚠ **Caution**
This defense is extremely CPU intensive and should be used with caution. Unrestricted use can cause a switch to halt operations should the CPU become overwhelmed with IP traffic. To prevent this, Allied Telesyn recommends activating this defense on only the uplink port and one other switch port at a time.

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 specified defense mechanism on a specified port.

Examples

The following command displays the IP address and subnet mask for the Land and SMURF defenses:

```
show dos ipaddress subnet
```

This command displays the status of the SMURF defense on port 4:

```
show dos smurf port=4
```

Chapter 25

STP Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the Spanning Tree Protocol (STP).

ACTIVATE STP

Syntax

```
activate stp
```

Parameters

None.

Description

Use this command to designate STP as the active spanning tree on the switch. 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 the switch at a time.

Example

The following command designates STP as the active spanning tree:

```
activate stp
```

DISABLE STP

Syntax

```
disable stp
```

Parameters

None.

Description

This command disables the Spanning Tree Protocol on the switch. The default setting for STP is disabled. To view the current status of STP, refer to SHOW STP on page 391.

Example

The following command disables STP:

```
disable stp
```

ENABLE STP

Syntax

```
enable stp
```

Parameters

None.

Description

This command enables the Spanning Tree Protocol on the switch. The default setting for STP is disabled. To view the current status of STP, refer to SHOW STP on page 391.

Note
You cannot enable STP until after you have activated it with ACTIVATE STP on page 380.

Example

The following command enables STP on the switch:

```
enable stp
```

PURGE STP

Syntax

```
purge stp
```

Parameters

None.

Description

This command returns all STP bridge and port parameters to the default settings. STP must be disabled in order for you to use this command. To disable STP, refer to DISABLE STP on page 381.

Example

The following command resets the STP parameter settings to their default values:

```
purge stp
```

SET STP

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 the following table. You specify the increment that represents the desired bridge priority value. The default value is 32,768 (increment 8).

Table 1 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

Table 1 Bridge Priority Value Increments (continued)

Increment	Bridge Priority	Increment	Bridge Priority
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. See ACTIVATE STP on page 380.

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
```

SET STP PORT

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. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

pathcost
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 for that LAN. 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 2 lists the STP port costs with Auto-Detect.

Table 2 STP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	100
100 Mbps	10
1000 Mbps	4

Table 3 lists the STP port costs with Auto-Detect when a port is part of a port trunk.

Table 3 STP 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. There are sixteen increments. The increments are listed in Table 4. You specify the increment of the desired value. The default is 128 (increment 8).

Table 4 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 configures the following STP parameter settings for a switch 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
```

This command sets the port cost to auto-detect on ports 7 to 10:

```
set stp port=7-10 portcost=auto
```

SET SWITCH MULTICASTMODE

Syntax

```
set switch multicastmode=a|b|c|d
```

Parameter

multicastmode Specifies one of the following:

a	Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all ports.
b	Forwards ingress spanning tree BPDU and 802.1x EAPOL packets across all VLANs and ports.
c	Forwards ingress BPDU and EAPOL packets only among the untagged ports of the VLAN where the ingress port is a member.
d	Forwards ingress BPDU and EAP packets on both tagged and untagged ports of the VLAN where the ingress port is a member.

Description

This command controls the behavior of the switch when forwarding ingress spanning tree BPDU packets and 802.1x port-based access control EAPOL packets when these features are disabled on the switch. Note the following when setting this parameter:

- ❑ You can only set this parameter from this command. You cannot configure it from the menus or web browser interface.
- ❑ The mode is set at the switch level. You cannot configure it on a per-port basis.
- ❑ A switch can have only one mode active at a time.
- ❑ The mode setting applies to spanning tree protocol BPDUs when STP, RSTP, and MSTP are disabled on the switch.
- ❑ The mode setting applies to 802.1x port-based access control EAPOL packets when 802.1x is disabled.

There are four possible states: A, B, C, and D. The states are described here:

A - Discards all ingress spanning tree BPDU and 802.1x EAPOL packets on all ports. The switch behaves as follows:

- ❑ If STP, RSTP, and MSTP are disabled, all ingress BPDUs are discarded.
- ❑ If 802.1x port-based access control is disabled, all ingress EAPOL packets are discarded.

B - Forwards ingress spanning tree BPDU and 802.1x EAPOL packets across all VLANs and ports. This is the default setting. The switch behaves as follows:

- ❑ If STP, RSTP, and MSTP are disabled, ingress BPDUs are flooded on all ports.
- ❑ If STP, RSTP, MSTP, and 802.1x are disabled on the switch, BPDUs and EAPOL packets are flooded on all ports.
- ❑ If the switch is running STP or RSTP and 802.1x is disabled, EAPOL packets are flooded on all ports, except ports in the blocking state.
- ❑ If the switch is running MSTP and 802.1x is disabled, EAPOL packets are flooded on all ports, including ports in the blocking state.

C - Forwards 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

The following command setting the switch’s mode to A to discard all ingress BPDUs and 802.1 EAPOL packets:

```
set switch multicastmode=a
```

SHOW STP

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.You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

Description

This command displays the current values for the following STP parameters:

- ❑ STP status
- ❑ Bridge identifier
- ❑ Bridge priority
- ❑ Hello time
- ❑ Forwarding delay
- ❑ Maximum age timer

You can also use this command to view the following STP parameter settings for a switch port:

- ❑ Port cost
- ❑ Port priority
- ❑ Port STP state

Examples

The following command displays the switch's STP settings:

```
show stp
```

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

```
show stp port=1-4
```

Chapter 26
RSTP Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the Rapid Spanning Tree Protocol (RSTP).

ACTIVATE RSTP

Syntax

```
activate rstp
```

Parameters

None.

Description

Use this command to designate RSTP as the active spanning tree on the switch. Once you have selected RSTP, you can enable or disable it using the ENABLE RSTP and DISABLE RSTP commands. RSTP is active on a switch 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 at a time.

Example

The following command designates RSTP as the active spanning tree:

```
activate rstp
```

DISABLE RSTP

Syntax

```
disable rstp
```

Parameters

None.

Description

This command disables the Rapid Spanning Tree Protocol on the switch. To view the current status of RSTP, use SHOW RSTP on page 404.

Example

The following command disables RSTP:

```
disable rstp
```

ENABLE RSTP

Syntax

```
enable rstp
```

Parameters

None.

Description

This command enables the Rapid Spanning Tree Protocol on the switch. The default setting for RSTP is disabled. To view the current status of RSTP, use SHOW RSTP on page 404.

You cannot enable RSTP until you have activated it with the ACTIVATE RSTP command.

Example

The following command enables RSTP:

```
enable rstp
```

PURGE RSTP

Syntax

```
purge rstp
```

Parameters

None.

Description

This command returns all RSTP bridge and port parameters to the default settings. RSTP must be disabled before you can use this command. To disable RSPT, refer to DISABLE RSTP on page 394.

Example

The following command resets RSTP:

```
purge rstp
```

SET RSTP

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 the following table. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 5 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

Table 5 Bridge Priority Value Increments

Increment	Bridge Priority	Increment	Bridge Priority
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
forceversion — Sets the RSTP mode. The parameters are equivalent. Values are:

stpcompatible — The bridge uses the RSTP parameter settings, but transmits only STP BPDU packets from the ports. This option is equivalent to the FORCESTPCOMPATIBLE option.

forcestpcompatible	The bridge uses the RSTP parameter settings, but transmits only STP BPDU packets from the ports. This option is equivalent to the STPCOMPATIBLE option.
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
- ❑ Port priority
- ❑ 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 393.

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
```

SET RSTP PORT

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]
```

Parameters

port
: Specifies the port you want to configure. You can specify more than one port at a time. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

pathcost
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 possible settings are:

cost
: A number for the port cost. The range is 1 to 200,000,000.

auto
: Automatically sets the port cost according to the speed of the port. This is the default. Table 6 lists the port cost with auto-detect.

Table 6 RSTP Auto-Detect Port Costs

Port Speed	**Port Cost**
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 7 lists the RSTP port costs with Auto-Detect when the port is part of a port trunk.

Table 7 RSTP Auto-Detect Port Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000
100 Mbps	20,000
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. There are sixteen increments. You specify the increment that corresponds to the desired value. The default is 128, which is increment 8.

Table 8 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. Options are:

yes, on, true

The port is an edge port. The values are equivalent. This is the default.

- no, off, false — The port is not an edge port. The values are equivalent.

ptp
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. Values are:

- yes, on, true — The port is an point-to-point port. The values 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 values are:

- yes, on, true — Enable migration check. The values are equivalent.
- no, off, false — Disable migration check. The values are equivalent.

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
```

SHOW RSTP

Syntax

```
show rstp [portconfig=port|portstate=port]
```

Parameters

portconfig — Displays the RSTP port settings. You can specify more than one port at a time.

portstate — Displays the RSTP port status. You can specify more than one port at a time.

Description

You can use this command to display the RSTP parameter settings. Values are displayed for the following parameters:

- ❑ RSTP status
- ❑ Bridge identifier
- ❑ Bridge priority
- ❑ Hello time
- ❑ Maximum aging
- ❑ Forwarding delay

You can also use this command to view the following RSTP parameter settings for a switch port:

- ❑ Port cost
- ❑ Port priority
- ❑ Edge and point-to-point status

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
```

Chapter 27

MSTP Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the Multiple Spanning Tree Protocol.

ACTIVATE MSTP

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
```

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 a MSTI.

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 410.

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 423.

Examples

This command associates the VLAN with the VID 4 to MSTI ID 8:

```
add mstp mstiid=8 mstivlanassoc=4
```

This command associates the VLANs with the VIDs 24 and 44 to MSTI ID 11:

```
add mstp mstiid=11 mstivlanassoc=24,44
```

CREATE MSTP

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 creates an MSTI ID and associates VLANs to the new spanning tree instance.

The MSTIID parameter specifies the new MSTI ID.

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 409 or SET MSTP MSTIVLANASSOC on page 423.

Examples

This command creates the MSTI ID 8 and associates to it the VLAN with the VID 4:

```
create mstp mstiid=8 mstivlanassoc=4
```

This 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
```

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 a VLAN from a spanning tree instance. A VLAN removed from a spanning tree instance is automatically returned 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

This command removes the VLAN with the VID 4 from MSTI ID 8:

```
delete mstp mstiid=8 mstivlanassoc=4
```

This command removes the VLANs with the VIDs 24 and 44 from MSTI ID 11:

```
delete mstp mstiid=11 mstivlanassoc=24,44
```

DESTROY MSTP MSTIID

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 a spanning tree instance. VLANs associated with a deleted MSTI are returned to CIST.

Example

This example deletes the spanning tree instance 4:

```
destroy mstp mstiid=4
```

DISABLE MSTP

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 429.

Example

The following command disables MSTP:

```
disable mstp
```

ENABLE MSTP

Syntax

```
enable mstp
```

Parameters

None.

Description

This command enables Multiple Spanning Tree Protocol on the switch. To view the current status of MSTP, refer to SHOW MSTP on page 429.

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 408

Example

The following command enables MSTP:

```
enable mstp
```

PURGE MSTP

Syntax

```
purge mstp
```

Parameters

None.

Description

This command returns all 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 408. To disable MSTP, refer to DISABLE MSTP on page 413.

Example

The following command resets the MSTP bridge and port parameter settings:

```
purge mstp
```

SET MSTP

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 RESET 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:

stpcompatible
: The bridge uses the MSTP parameter settings, but transmits only STP BPDU packets from the ports. This option is equivalent to the FORCESTPCOMPATIBLE option.

forcestpcompatible
: The bridge uses the MSTP parameter settings, but transmits only STP BPDU packets from the ports. This option is equivalent to the STPCOMPATIBLE option.

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.

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 decreased every time the BPDU crosses an MSTP regional boundary. Once the counter reaches zero, the BPDU is deleted.

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 level of an MSTP region. The range is 0 (zero) to 255. This is an arbitrary number that you assign to a region. The revision level must be the same on all bridges in a region. Different regions can have the same revision 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
```

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 the following table. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 9 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 in determining 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 429.

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 the following table. You specify the increment that represents the desired bridge priority value. The default value is 32,768, which is increment 8.

Table 10 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

This command changes the MSTI priority value to 45,056 (increment 11) for the MSTI ID 4:

```
set mstp msti mstiid=4 priority=11
```

This 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 410.

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 409.

Examples

This command associates the VLAN with the VID 4 to MSTI ID 8:

```
set mstp mstivlanassoc mstiid=8 vlanlist=4
```

This command associates VIDs 24 and 44 to MSTI ID 11:

```
set mstp mstivlanassoc mstiid=11 vlanlist=24,44
```

SET MSTP PORT

Syntax 1

```
set mstp port=port|all [extportcost=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. To configure all 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 11 lists the MSTP external port costs with the Auto setting when the port is not a member of a trunk.

Table 11 Auto External Path Costs

Port Speed	Port Cost
10 Mbps	2,000,000
100 Mbps	200,000
1000 Mbps	20,000

Table 12 lists the MSTP port costs with the Auto setting when the port is part of a port trunk.

Table 12 Auto External Path Trunk Costs

Port Speed	Port Cost
10 Mbps	20,000

Table 12 Auto External Path Trunk Costs

Port Speed	Port Cost
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
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 receiving 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 13 on page 426. You specify the increment of the desired value. The default is 128, which is increment 8.

Table 13 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.

Syntax 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
```

SHOW MSTP

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 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 MSTP settings for a port whose VLANs 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 can be used together with the PORTCONFIG and PORTSTATE parameters.

Description

This command displays MSTP parameters. For definitions of the MSTP terms used below, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

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

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
```

Chapter 28

VLANs and Multiple VLAN Mode Commands

This chapter contains the following commands:

Note
Remember to use the SAVE CONFIGURATION command to save your changes on the switch.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on tagged and port-based VLANs, multiple VLAN modes, and ingress filtering.

ADD VLAN

Syntax 1

```
add vlan=name [vid=vid] port=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 you want to modify.

vid — Specifies the VID of the VLAN you want to modify. This parameter is optional.

port — Specifies the ports to be added to the VLAN. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22).

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 create a new VLAN, see CREATE VLAN on page 435. To remove ports from a VLAN, see DELETE VLAN on page 439.

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.

Examples

The following command uses Syntax 1 to add ports 4 and 7 as untagged members to a VLAN called Sales:

```
add vlan=sales port=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 port=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 port=5 frame=tagged
add vlan=Service port=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
```

CREATE VLAN

Syntax 1

```
create vlan=name vid=vid port=ports|all
frame=untagged|tagged
```

Syntax 2

```
create vlan=name vid=vid 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.

port Specifies the ports on the switch that are either tagged or untagged members of the new VLAN. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-23), or both (for example, 1, 5, 14-22). To specify all ports on the switch, use ALL. This parameter must be followed by the FRAME parameter.

frame Specifies whether the ports of the VLAN are to be tagged or untagged. This parameter must be used with the PORT parameter.

taggedports Specifies the ports on the switch to serve as tagged ports in the VLAN. To specify all ports on the switch, use ALL. Omit this parameter if the VLAN does not contain tagged ports.

untaggedports Specifies the ports on the switch to function as untagged ports in the VLAN. To specify all ports on the switch, use ALL. Omit this parameter if the VLAN does not contain untagged ports.

Description

This command creates a new port-based or tagged VLAN.

This command has two syntaxes. You can use either syntax to create a port-based or tagged VLAN. The difference between the two syntaxes is how you specify which ports are members of the VLAN and whether the ports are tagged or untagged. 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 to which it is added. For instance, if you make port 4 an untagged member of a VLAN with a VID of 15, port 4’s PVID is changed to 15 automatically.

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.

Examples

The following command uses Syntax 1 to create a port-based VLAN called Sales with a VID of 3. The VLAN will consist of ports 4 to 8 and ports 12 to 16. All ports will be untagged ports in the VLAN:

```
create vlan=Sales vid=3 port=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 will consist of two tagged ports, ports 3 and 6:

```
create vlan=Production vid=22 port=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 port=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
```

That's the advantage of Syntax 2 over Syntax 1. You can create VLANs containing both types of ports with one rather than two commands.

DELETE VLAN

Syntax 1

```
delete vlan=name [vid=vid] port=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.
port	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 can remove both in the same command. This is illustrated in the Examples section below.

Note
To delete a VLAN, see DESTROY VLAN on page 442.

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.

Examples

The following command uses Syntax 1 to delete untagged ports 4 and 7 from a VLAN called Sales:

```
delete vlan=sales port=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 port=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 from the VLAN tagged port 2 and untagged ports 6 to 8, the commands would be:

```
delete vlan=Service port=2 frame=tagged
delete vlan=Service port=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
```

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

You can use this command, when the switch is operating in the user-configure VLAN mode, to delete port-based and tagged VLANs from a switch. You can use the command to deleted selected VLANS or to delete all VLANs, with the exception of the Default_VLAN.

When the switch is operating in the 802.1q-compliant mode, this command returns the switch back to the user-configure VLAN mode.

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
```

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 values are equivalent. This is the default.
no, off, false	Deactivates ingress filtering. The values 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 on page 68. For further information on ingress filtering, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

Example

The following command deactivates ingress filtering:

```
set switch infiltering=off
```

SET SWITCH MANAGEMENTVLAN

Syntax

```
set switch managementvlan=name|VID
```

Parameter

managementvlan	Specifies the management VLAN. You can specify the VLAN by name or by its VID. You can specify only one management VLAN. The default management VLAN is Default_VLAN (VID 1).

Description

This command sets the management VLAN. The switch uses this VLAN to watch for management packets from Telnet and web browser management sessions. For background information on the function of the management VLAN, refer to the *AT-S62 Management Software Menus Interface User's Guide*. To determine the current management VLAN, use the SHOW SWITCH command.

Example

The following command sets the TechSupport VLAN as the management VLAN:

```
set switch managementvlan=TechSupport
```

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.

Note
For background information on the multiple VLAN modes, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

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 448.

vid — Specifies the VID of the dynamic VLAN. To view VIDs, refer to SHOW VLAN on page 448. 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

Syntax

```
show vlan[=name|vid]
```

Parameter

vlan Specifies the name or VID of a VLAN.

Description

This command displays the following information:

- ❑ VLAN mode
- ❑ VLAN name
- ❑ Untagged port(s)
- ❑ Tagged port(s)

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
```

Chapter 29

GARP VLAN Registration Protocol Commands

This chapter contains the following commands:

- ❑ DISABLE GARP on page 450
- ❑ ENABLE GARP on page 451
- ❑ PURGE GARP on page 452
- ❑ SET GARP PORT on page 453
- ❑ SET GARP TIMER on page 454
- ❑ SHOW GARP on page 456
- ❑ SHOW GARP COUNTER on page 457
- ❑ SHOW GARP DATABASE on page 459
- ❑ SHOW GARP GIP on page 460
- ❑ SHOW GARP MACHINE on page 461

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the GVRP.

DISABLE GARP

Syntax

```
disable garp=gvrp [gip]
```

Parameters

garp	Specifies the GARP application you want to disable. The only GARP application supported by AT-S62 management software is GVRP.
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. Once disabled, the switch will not learn any new dynamic GVRP VLANs or dynamic GVRP ports. The default setting for GARP is disabled.

This command can also be used to disable GIP.

Note
Do not disable GIP if the switch is running GVRP. GIP is required for proper GVRP operation.

Examples

This command disables GVRP on the switch:

```
disable garp=gvrp
```

This command disables GIP only:

```
disable garp=gvrp gip
```

ENABLE GARP

Syntax

```
enable garp=gvrp [gip]
```

Parameters

garp	Specifies the GARP application you want to enable. The only GARP application supported by AT-S62 management software is GVRP.
gip	Enables GARP Information Propagation (GIP).

Note
The online help for this command contains an STP option. The option is not supported.

Description

This command enables GVRP on the switch. Once activated, the switch will learn dynamic GVRP VLANs and dynamic GVRP ports. The default setting for GARP is disabled.

This command can also be used to enable GIP. GIP must be enabled for GVRP to operate properly.

Examples

This commands enables GVRP on the switch:

```
enable garp=gvrp
```

This command enables GIP only:

```
enable garp=gvrp gip
```

PURGE GARP

Syntax

```
purge garp=gvrp
```

Parameter

garp	Specifies the GARP application you want to reset. The only GARP application supported by AT-S62 management software is GVRP.

Note
The online help for this command contains an STP option. The option is not supported.

Description

This command disables GVRP on the switch and returns the GVRP timers values to their default settings. All GVRP-related statistics counters are returned to zero.

Example

The following command disables GVRP and returns the timers to their default values:

```
purge garp=gvrp
```

SET GARP PORT

Syntax

```
set garp=gvrp port=port mode=normal|none
```

Parameters

garp — Specifies the GARP application you want to configure. The only GARP application supported by AT-S62 management software is GVRP.

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

mode — Specifies the GVRP mode of the port. Modes are:

normal — The port will participate in GVRP. The port will process GVRP information and transmit PDUs. This is the default.

none — The port will not participate in GVRP. The port will not process GVRP information nor transmit PDUs.

> **Note**
> The online help for this command contains an STP option. The option is not supported.

Description

This command sets a port's GVRP status. If you want a port to learn remote VLANs and transmit PDUs, set its mode to Normal. If you do not want a port to participate in GVRP, set its mode to None.

Examples

The following command deactivates GVRP on ports 1 to 4:

```
set garp=gvrp port=1-4 mode=none
```

The following command activates GVRP on port 3:

```
set garp=gvrp port=3 mode=normal
```

SET GARP TIMER

Syntax

```
set garp=gvrp timer [default] [jointime=integer]
[leavetime=integer] [leavealltime=integer]
```

Parameters

garp
Specifies the GARP application you want to configure. The only GARP application supported by AT-S62 management software is GVRP.

default
Returns the GARP timers to their default settings.

jointime
Specifies the Join Timer in centi seconds, 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 LeaveTimer in centi seconds, which are one hundredths of a second. The default is 60 centi seconds.

leavealltime
Specifies the LeaveAllTimer in centi seconds. The default is 1000 centi seconds.

Note
The online help for this command contains an STP option. The 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

The following command sets the Join Period timer to 0.1 second, Leave Period timer to 0.35 seconds, and the LeaveAllPeriod timer to 11 seconds for all GVRP applications:

```
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
```

SHOW GARP

Syntax

```
show garp=gvrp
```

Parameter

garp	Specifies the GARP application you want to display. The only GARP application supported by AT-S62 management software is GVRP.

Note
The online help for this command contains an STP option. The option is not supported.

Description

This command displays 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 Modes

Example

The following command displays the above GVRP information:

```
show garp=gvrp
```

SHOW GARP COUNTER

Syntax

```
show garp=gvrp counter
```

Parameter

garp — Specifies the GARP application you want to display. The only GARP application supported by AT-S62 management software is GVRP.

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 the above GARP counters:

```
show garp=gvrp counter
```

SHOW GARP DATABASE

Syntax

```
show garp=gvrp database
```

Parameters

garp	Specifies the GARP application you want to display. The only GARP application supported by AT-S62 management software is GVRP.

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 GARP database:

```
show garp=gvrp database
```

SHOW GARP GIP

Syntax

```
show garp=gvrp gip
```

Parameter

garp	Specifies the GARP application you want to display. The only GARP application supported by AT-S62 management software is GVRP.

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:

```
show garp=gvrp gip
```

SHOW GARP MACHINE

Syntax

```
show garp=gvrp machine
```

Parameter

garp	Specifies the GARP application you want to display. The only GARP application supported by AT-S62 management software is GVRP.

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:

```
show garp=gvrp machine
```

Chapter 30

Protected Ports VLAN Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
For background information on protected ports VLANs, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

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. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-22), or both (for example, 1, 5, 14-22). 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 466.
- ❑ 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 467.
- ❑ 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 467 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 467, 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 463.

Example

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 a protected ports VLAN. You can use this command to remove an uplink port or a port from a group.

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 untagged=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. You can specify the ports individually (for example, 5, 7, 22), as a range (for example, 18-22), or both (for example, 1, 5, 14-22).
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. The information includes the names and VIDs of the VLANs, and the tagged and untagged port members. If you are displaying a protected ports VLAN, the information also includes the group and port associations.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays the Sales VLAN:

```
show vlan=Sales
```

Chapter 31
MAC Address Security Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on port security.

SET SWITCH PORT INTRUSIONACTION

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. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

intrusionaction — Specifies the intrusion action. Options are:

discard	Discards an invalid frame. This is the default setting.
trap	Discards an invalid frame and sends an SNMP trap.
disable	Discards an invalid frame, sends an SNMP trap, and disables the port.

Description

This command changes the security intrusion action on a port that is operating in the Limited security mode. Intrusion action determines what a port will do when it receives an invalid frame.

Example

This command changes the intrusion action to trap on ports 12 and 21:

```
set switch port=12,21 intrusionaction=trap
```

SET SWITCH PORT SECURITYMODE

Syntax

```
set switch port=port
[securitymode=automatic|limited|secured|locked]
[intrusionaction=discard|trap|disable]
[learn=integer]
[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.You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

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, refer to ADD SWITCH FDB|FILTER on page 178.

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 SNMP trap.
disable	Discards invalid frames, sends an SNMP trap, and disables the port.

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. Options are:

yes, on, true	Enables the trap or disable intrusion action. These values are equivalent.
no, off, false	Disables the trap or disable intrusion action. The port still discards invalid ingress frames. This is the default. These values 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.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for explanations of the security levels and intrusion actions.

To view a port's current security mode, use the command SHOW SWITCH PORT SECURITYMODE on page 478.

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

This command sets the security level for port 8 to the Limited mode and specifies a limit of 5 dynamic MAC addresses. Since no intrusion action is specified, the discard action is assigned by default:

```
set switch port=8 securitymode=limited learn=5
```

This 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, nor to 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
```

SHOW SWITCH PORT INTRUSION

Syntax

```
show switch port=port intrusion
```

Parameters

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

This command displays the number of intrusion violations detected on ports 12 and 21:

```
show switch port=12,21 intrusion
```

SHOW SWITCH PORT SECURITYMODE

Syntax

```
show switch port=port securitymode
```

Parameters

port
Specifies the port whose security mode settings you want to view. You can specify more than one port at a time. You can specify the ports individually (for example, 5,7,22), as a range (for example, 18-23), or both (for example, 1,5,14-22).

Description

This command displays the security mode settings for the ports on the switch.

Example

This command displays the security mode settings for ports 1 to 5:

```
show switch port=1-5 securitymode
```

Chapter 32

802.1x Port-based Access Control Commands

This chapter contains the following commands:

- ❑ DISABLE PORTACCESS|PORTAUTH on page 480
- ❑ DISABLE RADIUSACCOUNTING on page 481
- ❑ ENABLE PORTACCESS|PORTAUTH on page 482
- ❑ ENABLE RADIUSACCOUNTING on page 483
- ❑ SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR on page 484
- ❑ SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT on page 489
- ❑ SET RADIUSACCOUNTING on page 491
- ❑ SHOW PORTACCESS|PORTAUTH on page 493
- ❑ SHOW PORTACCESS|PORAUTH PORT on page 494
- ❑ SHOW RADIUSACCOUNTING on page 495

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on 802.1x port-based access control.

DISABLE PORTACCESS|PORTAUTH

Syntax

```
disable portaccess|portauth
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

None.

Description

This command disables 802.1x Port-based Access Control on your switch. This is the default setting.

Example

The following command disables 802.1x Port-based Access Control on the switch:

```
disable portaccess
```

DISABLE RADIUSACCOUNTING

Syntax

```
disable radiusaccounting
```

Parameters

None

Description

This command disables RADIUS accounting on the switch. This command is equivalent to the SET RADIUSACCOUNTING STATUS=DISABLED command.

Example

The following command disables RADIUS accounting:

```
disable radiusaccounting
```

ENABLE PORTACCESS|PORTAUTH

Syntax

```
enable portaccess|portauth
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

None.

Description

This command activates 802.1x Port-based 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 you activate port-based access control. Refer to SET AUTHENTICATION on page 551.

Example

The following command enables 802.1x Port-based Access Control on the switch:

```
enable portaccess
```

ENABLE RADIUSACCOUNTING

Syntax

```
enable radiusaccounting
```

Parameters

None

Description

This command enables RADIUS accounting on the switch. This command is equivalent to the SET RADIUSACCOUNTING STATUS=ENABLED command.

Example

The following command disables RADIUS accounting:

```
enable radiusaccounting
```

SET PORTACCESS|PORTAUTH PORT ROLE=AUTHENTICATOR

Syntax

```
set portaccess|portauth port=port
type|role=authenticator|none
[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]
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

port

Specifies the port that you want 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
role

Specifies the role of the port. The parameters are equivalent. The role can be one of the following:

authenticator — Specifies the Authenticator role.

none — Disables port-based access control on the port.

control

Specifies the authenticator state. This parameter can take the following values:

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 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 forceunauthenticate	Causes the port to remain in the unauthorized state, ignoring all attempts by the client to authenticate. The switch cannot provide authentication services to the client through the interface. 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.	
reauthenabled	Controls whether the client must periodically reauthenticate. 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.

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.

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
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 65,535 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 the client logs on by providing a username and password combination. In the unauthorized state, the port will only accept EAP packets from the client. All other ingress packets that the port might receive from the client, including multicast and broadcast traffic, is discarded until the supplicant has logged on.

You can use this selection to control how an Authenticator port will handle 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 two selections are:

ingress An authenticator port, when in the unauthorized state, will discard all ingress broadcast and multicast packets from the client. while forwarding all egress broadcast and multicast traffic to the same client.

both An authenticator port, when in the unauthorized state, will not forward ingress or egress broadcast and multicast packets from or to the client until the client has logged on. This is the default.

piggyback Controls who can use the switch port in cases where there are multiple clients using the port (e.g., the port is connected to an Ethernet hub). 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.

Description

This command sets ports to the Authenticator role and configures the Authenticator role parameters. This command also disables port-based access control on a port.

Examples

This command sets ports 4 to 6 to the Authenticator role:

```
set portaccess port=4-6 role=authenticator
```

The following command sets port 7 to the Authenticator role. It sets the quiet period on the port to 30 seconds and the server timeout parameter to 200 seconds:

```
set portaccess port=7 role=authenticator
quietperiod=30 servtimeout=200
```

The following command disables port-based access control on ports 12 and 15:

```
set portaccess port=12,15 role=none
```

SET PORTACCESS|PORTAUTH PORT ROLE=SUPPLICANT

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 that 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
role — Specifies the role of the port. The parameters are equivalent. The role can be one of the following:

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 60 seconds. The default is 30 seconds.

heldperiod — Specifies the amount of time in seconds the supplicant is to refrain from retrying to re-contact the authenticator in the event the end user provides an invalid username and/or password. Once 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
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 64 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 contain 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 disables port-based access on a port.

Examples

This command sets ports 4 to 6 to the Supplicant role:

```
set portaccess port=4-6 role=supplicant
```

The following command sets port 8 to the Supplicant role. It sets the name to “switch22” and the password to “bluebird”:

```
set portaccess ports=8 role=supplicant
name=switch22 password=bluebird
```

The following command disables port-based access control on ports 12 and 15:

```
set portaccess port=12,15 role=none
```

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 deactivate RADIUS accounting on the switch. Options are:

- enabled — Activates RADIUS accounting. This option is equivalent to the ENABLE RADIUSACCOUNTING command.
- disabled — Deactivates the feature. This is the default. This option is equivalent to the DISABLE RADIUSACCOUNTING command.

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

This example activates RADIUS accounting and configures the software to send accounting information only when the user logs off:

```
set radiusaccounting status=enabled
trigger=stop_only
```

This example enables the update feature and sets the interval period to 200 seconds:

```
set radiusaccounting updateenable=enabled
interval=200
```

SHOW PORTACCESS|PORTAUTH

Syntax

```
show portaccess|portauth config|status
```

> **Note**
> The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

config	Displays whether port-based access control is enabled or disabled on the switch.
status	Displays the role and status of each port.

Description

Use this command to display operating information for port-based access control.

The CONFIG parameter displays:

- ❑ Enabled or disabled status of port-based access control
- ❑ Authentication method

The STATUS parameter displays the following information for each port:

- ❑ Port role
- ❑ Status

Examples

The following command displays whether port-based access control is enabled or disabled on the switch:

```
show portaccess config
```

This command displays the role and status for each port:

```
show portaccess status
```

SHOW PORTACCESS|PORAUTH PORT

Syntax

```
show portaccess|portauth port=port
authenticator|supplicant config|status
```

Note
The PORTACCESS and PORTAUTH keywords are equivalent.

Parameters

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.
status	Displays the status and role of the port.

Description

Use this command to display information about authenticator and supplicant ports.

Examples

The following displays the status for port 10, which has been set to the authenticator role:

```
show portaccess port=10 authenticator status
```

This command displays the port access configuration of port 12 which is a supplicant port:

```
show portaccess port=12 supplicant config
```

SHOW RADIUSACCOUNTING

Syntax

```
show radiusaccounting
```

Parameters

None.

Description

Use this command to display the current parameter settings for RADIUS accounting. For an explanation of the parameters, refer to SET RADIUSACCOUNTING on page 491.

Examples

The following command displays the current parameter settings for RADIUS accounting:

```
show radiusaccounting
```

Chapter 33

Web Server Commands

This chapter contains the following commands:

Note
Remember to use the SAVE CONFIGURATION command to save your changes.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the web server.

DISABLE HTTP SERVER

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 506. The default setting for the web server is enabled.

Example

The following command disables the web server:

```
disable http server
```

ENABLE HTTP SERVER

Syntax

```
enable http server
```

Parameters

None.

Description

This command activates the web server on the switch. Activating the server allows you to manage the unit from a web browser. To view the current status of the web server, see SHOW HTTP SERVER on page 506. The default setting for the web server is enabled.

Example

The following command activates the web server:

```
enable http server
```

PURGE HTTP SERVER

Syntax

```
purge http server
```

Parameters

None.

Description

This command resets the web server to its default values. Refer to the *AT-S62 Management Software Menus Interface User's Guide* for the web server default values. To view the current web server settings, refer to SHOW HTTP SERVER on page 506.

Example

The following command resets the web server parameters to the 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. Possible settings 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 default for non-secure HTTP operation is port 80. The default for secure HTTPS operation is port 443.

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 497.

❑ 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 to configuring 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 TIME on page 76 or you can configure the switch to obtain the date and time from an SNTP server using ADD SNTPSERVER PEER|IPADDRESS on page 71.
2. Create an encryption key pair using CREATE ENCO KEY on page 508 (syntax 1).
3. Create the self-signed certificate using CREATE PKI CERTIFICATE on page 518.
4. Add the self-signed certificate to the certificate database using ADD PKI CERTIFICATE on page 516.
5. Disable the switch's web server using DISABLE HTTP SERVER on page 497.
6. Configure the web server using SET HTTP SERVER on page 500.
7. Activate the web server using ENABLE HTTP SERVER on page 498.

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 an 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 the management software adds it automatically.) 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 steps to configuring the switch’s web server for CA certificates using the command line commands. The steps explain how to create an encryption key pair and an enrollment request, and how to load the CA certificates onto the switch:

1. Set the switch’s date and time. You can do this manually using the SET DATE TIME on page 76 or you can configure the switch to obtain the date and time from an SNTP server using ADD SNTPSERVER PEER|IPADDRESS on page 71.
2. Create an encryption key pair using CREATE ENCO KEY on page 508 (syntax 1).
3. Set the switch’s distinguished name using SET SYSTEM DISTINGUISHEDNAME on page 528.
4. Create an enrollment request using CREATE PKI ENROLLMENTREQUEST on page 521.
5. Upload the enrollment request from the switch to a management workstation or FTP server using UPLOAD METHOD=LOCAL on page 246.
6. Submit the enrollment request to a CA.
7. Once you have received the CA certificates, download them into the switch’s file system using LOAD METHOD=TFTP on page 238.

8. Add the CA certificates to the certificate database using ADD PKI CERTIFICATE on page 516.
9. Disable the switch's web server using the command DISABLE HTTP SERVER on page 497.
10. Configure the web server using SET HTTP SERVER on page 500.

11. Activate the web server using ENABLE HTTP SERVER on page 498

The following is an example of the command sequence for configuring the web server for a CA certificate. It explains how to create an encryption key pair and enrollment request, and how to download the CA certificates on the switch. (The example does not include step 1, setting the system time, nor the procedure for submitting the request to a CA, which will vary depending on the CA's enrollment requirements.)

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 a master switch's IP address of 149.44.44.44:

```
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 34

Encryption Key Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S62 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. For background information on encryption keys, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

CREATE ENCO KEY

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-S62 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. Possible settings 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-S62 file system to the key database.

Caution
Key generation is a CPU-intensive process. Because this process may affect switch behavior, Allied Telesyn 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 514.

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-S62 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-S62 file system, from where you can download it onto a management workstation 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. If you are importing a public key from the file system to the key database, the key ID that you select 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. To download files into the file system, refer to LOAD METHOD=TFTP on page 238.

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
```

DESTROY ENCO KEY

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. Once 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 514.

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 of 4:

```
destroy enco key=4
```

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 514.

The DESCRIPTION parameter specifies the new description for the key.

Example

This 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

Syntax

```
show enco key=key-id
```

Parameters

key	Specifies the ID of a key whose information you want to display.

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

This command displays information about encryption key 1:

```
show enco key=1
```

Chapter 35

Public Key Infrastructure (PKI) Certificate Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S62 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on Public Key Infrastructure certificates.

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. Possible settings 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 the type of certificate being added. Possible settings 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-S62 file system. To view the certificate files in the file system, refer to SHOW FILE on page 234. To view the certificates already in the database, refer to SHOW PKI CERTIFICATE on page 530.

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 530.

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, such as a public or private CA. The default is EE.

Note
The TRUSTED and TYPE parameters have no affect on the operation of a certificate on the switch. 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 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. Possible settings 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 518.

Once 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 516.

Note
For a review of the steps to configuring the web server for a self-signed certificate, refer to SET HTTP SERVER on page 500.

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 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 508. To view the IDs of the keys already on the switch, refer to SHOW ENCO on page 514.

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 Telesyn 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. For a explanation of distinguished names, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

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. Possible settings 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 518.

You must also set the system's distinguished name before using this command. For a explanation of distinguished names, refer to the *AT-S62 Management Software Menus Interface User's Guide*. To set the distinguished name, refer to SET SYSTEM DISTINGUISHEDNAME on page 528.

Note
For a review of all the steps to configuring the web server for a CA certificate, refer to SET HTTP SERVER on page 500.

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.

Examples

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 530.

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 230.

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 will consider the certificate as 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 230.

Example

```
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. Possible settings 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. Possible settings 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 530.

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 530.

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 on the switch. You can select any permitted value for either parameter. The parameters are included only as placeholders for information in the certificate database.

Example

This 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 that can be stored in the certificate database. The range is 12 and 256; the default is 256.

Description

This command sets the maximum number of certificates that can be stored in the switch's certificate database.

Example

This 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. For a explanation of distinguished names, refer to the *AT-S62 Management Software Menus Interface User’s Guide*.

Allied Telesyn 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, which do not have an IP address, you can use the IP address or domain name of the master switch of the enhanced stack as the 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 518, 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 521.

Example

This 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 527.

Example

```
show pki
```

SHOW PKI CERTIFICATE

Syntax

```
show pki certificate[=”name”]
```

Parameter

certificate	Specifies the name of the certificate whose information you want to view. 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

This command lists all of the certificates in the database:

```
show pki certificate
```

This command displays information specific to the certificate “Switch 12 certificate”:

```
show pki certificate=”Switch 12 certificate”
```

Chapter 36

Secure Sockets Layer (SSL) Commands

This chapter contains the following command:

- ❑ SET SSL on page 532
- ❑ SHOW SSL on page 533

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S62 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on SSL.

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 second.
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 second.

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

```
show ssl
```

Chapter 37
Secure Shell (SSH) Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
The feature is not available in all versions of the AT-S62 management software. Contact your Allied Telesyn sales representative to determine if this feature is available in your locale. For background information on SSH, refer to the *AT-S62 Management Software Menus Interface User's Guide*.

DISABLE SSH SERVER

Syntax

```
disable ssh server
```

Parameters

None.

Description

This command disables the Secure Shell server. When the Secure Shell server is disabled, connections from Secure Shell clients are not accepted.

By default, the Secure Shell server is disabled.

Example

The following command disables the Secure Shell server:

```
disable ssh server
```

ENABLE SSH SERVER

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, connections from Secure Shell clients are accepted. 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 508 (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 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 40.

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 508.
2. Disable Telnet access to the switch with the DISABLE TELNET command. See DISABLE TELNET on page 40.

   Although the AT-S62 management software allows the SSH and Telnet servers to be active on the switch simultaneously, allowing Telnet to remain active negates the security of the SSH feature.
3. Configure and activate SSH on the switch using ENABLE SSH SERVER on page 536.
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. Logon 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. You can add, delete, and modify users with the RADIUS and TACACS+ feature. For information about how to configure RADIUS and TACACS+, see TACACS+ and RADIUS Commands on page 542.

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
   ```

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 508 (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

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
```

Chapter 38

TACACS+ and RADIUS Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the RADIUS and TACACS+ authenticator protocols.

ADD RADIUSSERVER

Syntax

```
add radiusserver server|ipaddress=ipaddress
order=value [secret=string] [port=value]
[accport=value]
```

Parameters

server 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.

port — Specifies the UDP (User Datagram Protocol) port of the RADIUS server. The default is port 1812.

accport — Specifies the UDP (User Datagram Protocol) port for RADIUS accounting. The default is port 1813.

Description

Use this command to add the IP addresses of 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.

Examples

The following command adds the RADIUS server with the IP address 149.245.22.22 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 as the third RADIUS server to be queried by the switch.

```
add radiusserver ipaddress=149.245.22.22 order=3
```

The following command adds the RADIUS server with the IP address 149.245.22.22. It specifies the order as 2 and the encryption key as tiger74.

```
add radiusserver ipaddress=149.245.22.22 order=2
secret=tiger74 port=1812
```

ADD TACACSSERVER

Syntax

```
add tacacsserver server|ipaddress=ipaddress
order=value [secret=string]
```

Parameters

server
ipaddress
Specifies an IP address of a TACACS+ server. The parameters are equivalent.

order
Specifies the order that your TACACS+ servers are queried by the switch. You can assign order to up to 3 servers with 1 being the first server queried.

secret
Specifies the optional encryption key used on this server.

Description

Use this command to add the IP addresses of TACACS+ servers to your switch along with the order the TACACS+ servers are to be queried and an optional encryption key.

Examples

The following command adds a TACACS+ server with an IP address 149.245.22.20 and an order value of 1:

```
add tacacsserver ipaddress=149.245.22.20 order=1
```

The following command adds a TACACS+ server with an IP address of 149.245.22.24, an order of 2, and an encryption code of lioness54:

```
add tacacsserver ipaddress=149.245.22.24 order=2
secret=lioness54
```

The following command adds a TACACS+ server with an IP address 149.245.22.26. It specifies this TACACS+ server as the third TACACS+ server to be queried by the switch.

```
add tacacsserver ipaddress=149.245.22.26 order=3
```

DELETE RADIUSSERVER

Syntax

```
delete radiusserver server|ipaddress=ipaddress
```

Parameter

server
ipaddress Specifies the IP address of a RADIUS server to be deleted from the management software. The parameters are equivalent.

Description

Use this command to delete the IP address of a RADIUS from your switch.

Example

The following command deletes the RADIUS server with the IP address 149.245.22.22:

```
delete radiusserver ipaddress=149.245.22.22
```

DELETE TACACSSERVER

Syntax

```
delete tacacsserver server|ipaddress=ipaddress
```

Parameter

server ipaddress	Specifies the IP address of a TACACS+ server to be deleted from the management software. The parameters are equivalent.

Description

Use this command to delete the IP address of a TACACS+ server from your switch.

Example

The following command deletes the TACACS+ server with the IP address 149.245.22.20:

```
delete tacacsserver ipaddress=149.245.22.20
```

DISABLE AUTHENTICATION

Syntax

```
disable authentication
```

Parameters

None.

Description

Use this command to disable TACACS+ and RADIUS manager account authentication on your switch. When you disable authentication you retain your current authentication parameter settings.

Note
This command applies only to TACACS+ and RADIUS manager accounts. Once disabled, 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. If you are using the RADIUS authentication protocol for port-based access control but not for manager account authentication, you can leave authentication disabled and the switch will still be able to access the RADIUS configuration information for 802.1x port-based access control.

Example

The following command disables TACACS+ and RADIUS authentication on your switch:

```
disable authentication
```

ENABLE AUTHENTICATION

Syntax

```
enable authentication
```

Parameters

None.

Description

Use this command to activate TACACS+ or RADIUS manager account authentication on your switch. Once the feature is enabled, you can use the manager accounts you created on the authentication server to log on and manage the switch.

> **Note**
> This command does not affect 802.1x port-based access control. If you are using the RADIUS authentication protocol for port-based access control but not for manager account authentication, you can leave authentication disabled and the switch will still be able to access the RADIUS configuration information for 802.1x port-based access control.

Example

The following command activates manager account authentication on your switch:

```
enable authentication
```

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 address or secret of any RADIUS or TACACS+ authentication servers you may have specified.

Example

The following command disables authentication on your switch:

```
purge authentication
```

SET AUTHENTICATION

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 that is used by 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 545 or ADD RADIUSSERVER on page 543.

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. Once the switch has exhausted the list of servers, the switch defaults to the standard Manager and Operator accounts. The default is 10 seconds. The range is 1 to 60 seconds.

Description

Use this command to select the authentication protocol. One one authentication protocol can be active on the switch at a time. You may specify a global encryption code and the maximum number of seconds the switch waits for a response from an authenticator server.

Examples

The following command selects TACACS+ as the authentication protocol on the switch:

```
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
```

SHOW AUTHENTICATION

Syntax

```
show authentication[=tacacs|radius]
```

Parameters

None.

Description

This command displays the following information about the authenticated protocols on the switch:

- ❑ Status - The status of the authenticated protocol: enabled or disabled. The default is disabled.
- ❑ Authentication Method - The authentication protocol activated on the switch: TACACS+ or RADIUS. The default is the TACACS+ protocol.
- ❑ The IP addresses of up to three 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 authentication protocol information on your switch:

```
show authentication
```

The following command displays the information for the RADIUS protocol:

```
show authentication=radius
```

Chapter 39

Management ACL Commands

This chapter contains the following commands:

Note
Remember to save your changes with the SAVE CONFIGURATION command.

Note
Refer to the *AT-S62 Management Software Menus Interface User's Guide* for background information on the Management ACL.

ADD MGMTACL

Syntax

```
add mgmtacl ipddress=ipaddress mask=string
protocol=tcp interface=telnet|web|all
```

Parameters

ipaddress Specifies the IP address of a specific management workstation or a subnet.

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, in the IPADDRESS parameter, you specified the IP address of a specific management workstation, the appropriate mask is 255.255.255.255. If you are filtering on a subnet, then the mask would depend on the subnet address. For example, for a Class C subnet address of 149.11.11.32, the mask would be 255.255.255.224.

protocol Specifies the protocol of the management packets. The only permitted selection is TCP.

interface Specifies the type of remote management allowed. The options are:

telnet	Telnet management
web	Web management
all	Both Telnet and web management

Description

This command adds an access control entry to the Management ACL. There can be up to 256 ACEs in the Management ACL.

An ACE is an implicit "permit" statement. A workstation that meets the criteria of an ACE will be allowed to remotely manage the switch.

The IPADDRESS parameter specifies the IP address of a specific management workstation 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, the mask will depend on the subnet. For example, to allow all management workstations in the subnet 149.11.11.0 to manage the switch, you would enter the mask 255.255.255.0.

The PROTOCOL parameter has only the one setting TCP. This is because Telnet and web browser management packets for an AT-8500 Series switch are exclusively TCP.

The INTERFACE parameter allows you control whether the remote management station can manage the switch using Telnet, a web browser, or both. 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 to add an entry.

Example

The following command allows the management workstation with the IP address 169.254.134.247 to manage the switch from either a Telnet or web browser management session:

```
add mgmtacl ipaddress=169.254.134.247
mask=255.255.255.255 protocol=tcp interface=all
```

The following command allows the management workstation with the IP address 169.254.134.12 to manage the switch using only a web browser:

```
add mgmtacl ipaddress=169.254.134.12
mask=255.255.255.255 protocol=tcp interface=web
```

The following command allows all management workstations in the subnet 169.24.144.32 to manage the switch using a Telnet protocol application:

```
add mgmtacl ipaddress=169.24.144.32
mask=255.255.255.224 protocol=tcp
interface=telnet
```

DELETE MGMTACL

Syntax

```
delete mgmtacl ipaddress=ipaddress mask=string
protocol=tcp interface=telnet|web|all
```

Parameters

ipaddress Specifies the IP address of the ACE to be deleted.

mask Specifies the ACE's mask.

protocol Specifies the ACE's protocol. There is only one option:

tcp	Transmission control protocol.

interface Specifies the ACE's management method. The options are:

telnet	Telnet management
web	Web management.
all	Both Telnet and web management.

Description

This command deletes an ACE from the Management ACL. You must enter all the parameters to delete an entry. To view the entries in the Management ACL, refer to SHOW MGMTACL on page 563.

Example

The following command deletes an ACE from the Management ACL:

```
delete mgmtacl ipaddress=169.254.134.247
mask=255.255.255.255 protocol=tcp interface=all
```

DISABLE MGMTACL

Syntax

```
disable mgmtacl
```

Parameters

None

Description

This command disables the Management ACL. This command is equivalent to the SET MGMTACL STATE=DISABLE command.

Example

The following command disables the Management ACL.

```
disable mgmtacl
```

ENABLE MGMTACL

Syntax

```
enable mgmtacl
```

Parameters

None

Description

This command enables the Management ACL. This command is equivalent to the SET MGMTACL STATE=ENABLE command.

> **Note**
> Activating the Management ACL without entering any access control entries (ACEs) prohibits you from remotely managing the switch from a Telnet or web browser management session.

Example

The following command enables the Management ACL.

```
enable mgmtacl
```

SET MGMTACL

Syntax

```
set mgmtacl ipaddress=ipaddress mask=string
protocol=tcp interface=telnet|web|all
```

Parameters

ipaddress	Specifies the IP address of the ACE to be modified.	
mask	Specifies the ACE's mask.	
protocol	Specifies the ACE's management protocol. This parameter supports only one option:	
	tcp	Transmission control protocol.
interface	Specifies the new management method for the ACE. The options are:	
	telnet	Telnet management
	web	Web management.
	all	Both Telnet and web management.

Description

This command changes the management method of an existing management access control entry in the Management ACL. For instance, you might use this command to change an entry from Telnet management only to both Telnet and web browser management.

You cannot change the IP address or subnet mask of an existing entry in the table using this command. Changing these parameters requires deleting the entry and reentering it with the necessary corrections.

Note
You must specify all the parameters when modifying the management method of an ACE.

Example

The following command changes an existing access control entry with an IP address of 169.254.134.247 and a subnet mask of 255.255.255.255 to permit web browser management only:

```
set mgmtacl ipaddress=169.254.134.247
mask=255.255.255.255 protocol=tcp interface=web
```

SET MGMTACL STATE

Syntax

```
set mgmtacl state=disable|enable
```

Parameters

state Sets the state of the Management ACL. The options are:

enable	Enables the Management ACL.
disable	Disables the Management ACL. This is the default setting.

Description

This command enables or disables the Management ACL. This command is equivalent to the ENABLE MGMTACL and DISABLE MGMTACL commands.

Note
Activating the Management ACL without entering any access control entries (ACEs) prohibits you from remotely managing the switch from a Telnet or web browser management session.

Example

The following command enables the Management ACL:

```
set mgmtacl state=enable
```

SHOW MGMTACL

Syntax

```
show mgmtacl state|entries
```

Parameters

state Displays the status of the Management ACL as either enabled or disabled.

entries Lists the entries in the Management ACL.

Description

This command shows the state of and entries in the Management ACL. You can specify only one parameter at a time.

Examples

The following command displays whether the Management ACL is enabled or disabled.

```
show mgmtacl state
```

The following command displays the ACEs in the Management ACL:

```
show mgmtacl entries
```

Index