Management Software

AT-S39

♦

Command Line User's Guide

AT-8012M, AT-8012M-QS, AT-8016F/xx (MT, SC and ST), AT-8024, AT-8024GB, AT-8024M, AT-8026FC, AT-8026T, and AT-8088/xx (MT and SC) FAST ETHERNET SWITCHES

VERSION 3.3.0

Allied Telesyn

Table of Contents

Preface

This guide contains instructions on how configure an AT-8000 Series Fast Ethernet Switch using the AT-S39 command line interface.

The AT-8000 Series consists of the following Fast Ethernet switches:

❑ AT-8012M

❑ AT-8012M-QS

❑ AT-8016F/xx (MT, SC and ST)

❑ AT-8024

❑ AT-8024GB

❑ AT-8024M

❑ AT-8026FC

❑ AT-8026T

❑ AT-8088/xx (MT and SC)

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.

Where to Find Web-based Guides

The installation and user guides for all Allied Telesyn products are available in Portable Document Format (PDF) from on our web site at www.alliedtelesyn.com. You can view the documents on-line or download them onto a local workstation or server.

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: **http://kb.alliedtelesyn.com**. 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: **http://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: **http://www.alliedtelesyn.com**.

For Sales or Corporate Information   You can contact Allied Telesyn for sales or corporate information at our web site: **http://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: **http://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 sections:

Starting a Management Session

To manage an AT-8000 Series switch using the command line commands, you must first start a local or Telnet management session. For instructions on how to start a management session, refer to the **AT-S39 Management Software User's Guide**.

Note
The command line interface is not supported from a web browser management session.

Once you have started a management session, you will see the AT-S39 Main Menu. This menu includes the following option as one of its selections:

```
C – Command Line Interface
```

Type **C** to display the command line prompt. The prompt will differ depending on the management account you used to log onto the switch. If you logged in as manager, the prompt is "Manager::$". If you logged in as operator, the prompt is "Operator::$". You can now manage the switch with the command line commands.

Key Features

The following features are supported in the command line interface:

❑ Command history using the up and down arrow keys. (Not supported in a Telnet management session.)

❑ Context-specific help - Type a question mark at any time to see a list of legal next parameters.

❑ Keyword abbreviations - Any keyword can be recognized just by typing an unambiguous prefix (e.g., "sh" for "show"). These prefixes are indicated by capital letters in the screen text representation of the commands.

❑ Tab key - Pressing the tab key completes 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 is used for command formats and examples.

❑ *`screen text font`* - Italicized screen text indicates a variable for you to enter.

❑ [ ] - Brackets indicate optional parameters.

❑ | - The bar symbol separates parameter options from which you must choose.

Chapter 2
Basic Command Line 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
```

HELP

Syntax

```
help
```

Parameters

None.

Description

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

Example

The following command displays the command keywords:

```
help
```

LOGOFF and QUIT

Syntax

```
logoff
quit
```

Parameters

None.

Description

Both 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 on 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-S39 Main Menu. For instructions on how to use the management menus, refer to the **AT-S39 Management Software User's Guide**.

Example

The following command displays the AT-S39 Main Menu:

```
menu
```

SAVE CONFIGURATION

Syntax

```
save configuration
```

Parameters

None.

Description

This command saves your changes to the switch's flash memory for permanent storage.

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

To save your changes, you must use this command. Your changes are saved to flash memory and are retained even when the switch is reset or powered off.

Example

The following command saves your configuration:

```
save configuration
```

SET PROMPT

Syntax

set prompt="*prompt*"

Parameter

Prompt   Specifies the command line prompt. The prompt can be from one to fifteen alphanumeric characters. Spaces are allowed. If spaces are included, the prompt must be enclosed in double quotes. Otherwise, the quotes are optional.

Description

This command changes the command prompt. Assigning each switch a different command prompt will make it easier for you to distinguish between the switches and help prevent you from performing a configuration procedure on the wrong switch. The default command prompts are Manager::$ and Operator::$.

Example

The following command changes the command prompt to "Switch7".

```
set prompt=Switch7
```

SET SWITCH CONSOLEMODE

Syntax

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

Parameter

consolemode   Specifies the mode you want management sessions to start in. Options are:

cli   Starts a management session with the command line prompt.

menu   Starts a management session with the AT-S39 Main Menu.

Description

You can use this command to specify whether you want your management sessions to display the command line interface or the menu interface when you start a session. The default is the menu interface.

Example

The following command configures the management software to always display the command line prompt when you start a management session:

```
set switch consolemode=cli
```

SHOW USER

Syntax

```
show user
```

Parameters

None.

Description

This command displays the manager account username you used to log onto the switch.

Chapter 3
Basic Switch Commands

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

DISABLE DHCPBOOTP

Syntax

```
disable dhcpbootp
```

Parameters

None.

Description

This command deactivates the DHCP and BOOTP client software on the switch.

Example

The following command deactivates DHCP and BOOTP:

```
disable dhcpbootp
```

ENABLE DHCPBOOTP

Syntax

```
enable dhcpbootp
```

Parameters

None.

Description

This command activates the DHCP and BOOTP client software on the switch. When activated, this software instruct the switch to obtain its IP configuration from a DHCP or BOOTP server on your network, whenever the unit is power cycled or reset. The switch will make continuous requests for its IP configuration until a DHCP or BOOTP server responds.

If you have assigned the switch an IP address manually, the address is discarded when DHCP and BOOTP are activated.

The default setting for the DHCP and BOOTP client software is disabled.

> **Note**
> You cannot manually assign an IP address or subnet mask to a switch once the DHCP and BOOTP client software have been activated. To disable DHCP and BOOTP, refer to the DISABLE DHCPBOOTP command.

Example

The following command activates the DHCP and BOOTP client software:

```
enable dhcpbootp
```

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.

Example

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

```
ping 149.245.22.22
```

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 255.255.0.0.

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 with this command you can specify which parameter to reset, while you cannot with the RESET IP command.

Example

The following command returns the switch's IP address and subnet mask to their default values:

```
purge ip ipaddress netmask
```

RESET IP

Syntax

```
reset ip interface=1
```

Parameter

interface   Specifies the interface number. This value is always "1".

Description

This command returns a switch's IP address, subnet mask, and gateway address to the default values.

To return just one parameter to its default value, refer to the PURGE IP command.

Example

The following command returns the switch's IP address, subnet mask, and gateway address to their default values:

```
reset ip interface=1
```

RESET SYSTEM

Syntax

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

Parameters

name   Deletes the name of the switch.

contact   Deletes the name of the network administrator
                      responsible for managing the unit.

location   Deletes the location of the switch.

Description

This command deletes the information listed above in Parameters.
Omitting the parameters deletes all three items from the switch.

To set the name, contact, and location information for a switch, refer to
the SET SYSTEM command. To display the information, use the SHOW
SYSTEM command.

Examples

The following command deletes all three items:

```
reset system
```

The following command deletes just the location:

```
reset system location
```

RESTART REBOOT

Syntax

```
restart reboot
```

Parameters

None.

Description

This command returns the switch's operating parameters to the default settings.

⚠️ **Caution**

This command involves a switch reset. Some network traffic may be lost.

Example

The following command returns the switch's operating parameters to the default settings:

```
restart reboot
```

Follow the prompts.

RESTART SWITCH

Syntax

```
restart switch
```

Parameter

None.

Description

This command resets the switch. The system reset will take only a few seconds. The unit will not forward traffic during time required to reload the 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 changes not saved will be lost.

Example

The following command resets the switch:

```
restart switch
```

SET IP

Syntax

```
set ip interface=1 ipaddress=ipaddress|DHCP
netmask=subnetmask
```

Parameters

interface   Specifies the interface number. This value is always "1".

ipaddress   Specifies an IP address for the switch or activates DHCP and BOOTP. The default value is 0.0.0.0.

netmask   Specifies the subnet mask for the switch. The default value is 0.0.0.0. You must specify a subnet mask if you manually assigned the switch an IP address.

Description

This command configures the following switch parameters:

❑ IP address

❑ Subnet mask

For background information on when to assign a switch an IP address, refer to the **AT-S39 Management Software User's Guide**.

This command can also be used to activate the DHCP and BOOTP client software on the switch. Activating DHCP and BOOTP with this command is equivalent to the ENABLE DHCPBOOTP command.

> **Note**
> You cannot assign an IP address to the switch if the DHCP and BOOTP client software is enabled. To deactivate DHCP and BOOTP, refer to the DISABLE DHCPBOOTP command.

To view the switch's current IP and subnet mask settings, refer to the SHOW IP command. To return the IP address and subnet mask to their default values, refer to the PURGE IP command or the RESET IP command.

To view the status of the DHCP and BOOTP client software, refer to SHOW DHCPBOOTP command.

Examples

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

```
set ip interface=1 ipaddress=140.35.22.22
netmask=255.255.255.0
```

The following command sets just the subnet mask:

```
set ip interface=1 netmask=255.255.255.210
```

The following command activates the DHCP and BOOTP client software:

```
set ip interface=1 ipaddress=dhcp
```

SET IP ROUTE

Syntax

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

Parameter

ipaddress   Specifies the IP address of the default gateway for the switch. The default value is 0.0.0.0.

Description

This command specifies the IP address of the default gateway for the switch. This address is required if you will be managing the unit from a remote management station that is separated from the switch by a router.

To view the switch's current default gateway address settings, refer to the SHOW IP command. To return the parameter to its default value, refer to the PURGE IP command or the RESET IP command.

Example

The following command sets the default gateway address to 140.35.22.12:

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

SET SYSTEM

Syntax

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

Parameters

The parameters are defined below:

name   Specifies the name of the switch. The name can be from 1 to 30 alphanumeric characters in length and must be enclosed in quotes (" ").

contact   Specifies the name of the network administrator responsible for managing the switch. The contact can be from 1 to 30 alphanumeric characters in length and must be enclosed in quotes (" ").

location   Specifies the location of the switch. The location can be from 1 to 30 alphanumeric characters in length and must be enclosed in quotes (" ").

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.

To view the current settings for these parameters, refer to the SHOW SYSTEM command. To delete the current settings without applying new settings, refer to the RESET SYSTEM command.

Example

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"
```

SHOW CONFIG

Syntax

```
show config
```

Parameters

None.

Description

This command displays overall information on the switch and the ports.

Example

The following command displays information about the switch and the ports:

```
show config
```

SHOW DHCPBOOTP

Syntax

```
show dhcpbootp
```

Parameters

None.

Description

This command displays the status of the DHCP and BOOTP client software on the switch. The client software will be either "enabled" or "disabled." When enabled, the switch obtains its IP configuration information from a DHCP or BOOTP server on the network. The default setting is disabled.

To enable the client software, refer to the ENABLE DHCPBOOTP command. To disable it, refer to the DISABLE DHCPBOOTP command.

Example

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

```
show dhcpbootp
```

SHOW IP

Syntax

```
show ip interface=1
```

Parameters

interface   Specifies the interface number. This value is always "1".

Description

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

❑ IP address

❑ Subnet mask

❑ Default gateway

To set these parameters, refer to the SET IP and the SET IP ROUTE commands.

Example

The following command displays the values of several switch parameters:

```
show ip interface=1
```

SHOW IP ROUTE

Syntax

```
show ip route
```

Parameters

None.

Description

This command displays the switch's default gateway address.

To set this parameter, refer to the SET IP ROUTE command.

Example

The following command displays the default gateway address:

```
show ip route
```

SHOW SWITCH

Syntax

```
show switch
```

Parameters

None.

Description

This command displays the following switch parameters:

❑ MAC address

❑ MAC aging time

❑ VLAN mode and status

❑ Management VLAN

❑ Ingress filtering status

❑ Enhanced stacking status

❑ Console startup mode

❑ Console disconnect timer

❑ Security mode

❑ Port mirrors

❑ Broadcast timers

❑ Port mirror

❑ Spanning tree version

Example

The following command displays the above information:

```
show switch
```

SHOW SYSTEM

Syntax

`show system`

Parameters

None.

Description

This command displays the following information:

❑ Application software version and build date

❑ Bootloader version and build date

❑ Serial number

❑ Model name

❑ Switch's name

❑ Name of the network administrator responsible for managing the unit

❑ Location of the unit.

Note
For instructions on how to set this information, see the SET SYSTEM command. For instructions on how to remove the information, see the RESET SYSTEM command.

Example

The following command displays information about the switch:

`show system`

Chapter 4
Enhanced Stacking Commands

❑ **ACCESS SWITCH** on page 45

❑ **EXIT** on page 46

❑ **SET SWITCH STACKMODE** on page 47

❑ **SHOW REMOTELIST** on page 48

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

Note
Refer to the **AT-S39 Management Software 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 can view this
                    number using the SHOW REMOTELIST command.

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

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

Description

You use this command to start a management session on another switch
in an enhanced stack. You can specify the switch by switch number or by
MAC address., both displayed with the SHOW REMOTELIST command.
You must perform the SHOW REMOTELIST command before you can
access a switch with the ACCESS SWITCH command.

> **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 a switch, use the SHOW SWITCH
> command.

Examples

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

```
access switch number=12
```

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

```
access switch macaddress=003084520211
```

EXIT

Syntax

```
exit
```

Parameters

None.

Description

Ends a management session. The menu or screen that is displayed as a result of this command depends on whether your switch is a master or slave as well as the configuration of the console mode on your switch. If you have configured your switch with the command line as the console mode, entering the EXIT command ends the management session. For a master switch, this command actually disconnects the session. However, for a slave switch, the EXIT command ends the slave session and displays the Stacking Services Menu on the master switch.

If you have left the console mode configured as menu, when you enter the EXIT command the AT-S39 Main Menu is displayed. For a master switch, the AT-S39 Main Menu of the master switch is displayed. For a slave switch, the AT-S39 Main Menu of the slave switch is displayed.

> **Note**
> To determine the master or slave status of your switch, use the SHOW SWITCH command.

Example

The following command end a management session:

```
exit
```

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 RS232 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 a switch's current stacking status, refer to the SHOW SWITCH command.

> **Note**
> You cannot change the stacking status of a switch accessed 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 set the 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]
```

Parameters

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

Description

This command displays a lists of the switches in an enhanced stack. 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 function from a management session of a slave switch. To determine the master or slave status of your switch, use the SHOW SWITCH command.

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 by=name
```

Chapter 5

SNMP Community Strings and Trap Commands

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

ADD SNMP COMMUNITY TRAPHOST

Syntax

```
add snmp community="community" traphost=ipaddress
```

Parameters

community   Specifies the switch's SNMP Read or Write community string. The string 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.

traphost   Specifies the IP address of a management workstation to receive management traps from the switch.

Description

You can use this command to specify the IP address of a management workstation to receive management traps from the switch. The switch can support up to four IP addresses of trap receivers, but only one can be added at a time with this command.

To use this command, you must specify the switch's Read or Write community string. You can specify either string.

To view the current community strings or to see if any management workstation IP addresses have already been assigned, use the SHOW SNMP command.

Example

The following command adds the IP address 149.212.11.22 of a management workstation to receive traps from the switch. It uses the default SNMP Read access community string "public".

```
add snmp community=public traphost=149.212.11.22
```

CREATE SNMP COMMUNITY

Syntax

```
create snmp community="community"
access=read|write [traphost=ipaddress]
```

Parameter

community   Specifies the new community string. A community string can be up to thirteen characters. Community strings are case sensitive. If the string contains a space or special character, such as an exclamation point, it must be enclosed in double quotes; otherwise, the quotes are optional.

access   Specifies the string's access level. Options are Read and Write.

traphost   Specifies the IP address of a management workstation to receive management traps from the switch.

Description

This command creates a new Read or Write community string on the switch.

The switch supports only one Read community string and one Write community string at a time. Consequently, you cannot create a new Read or Write community string until after you have deleted the current community string using the DESTROY SNMP command. For example, to create a new community string with Read access, you must first destroy the current community string that has that access level. To view the current community strings, refer to the SHOW SNMP command.

When you create a new community string, you can specify an IP address of a network node to receive traps from the switch, referred to as a trap receiver. The switch can support up to four IP addresses of trap receivers, but only one can be added with this command. To add more IP addresses of trap receivers, refer to the ADD SNMP COMMUNITY TRAPHOST command.

Example

The following command creates the new Read community sting "serv12":

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

DELETE SNMP COMMUNITY TRAPHOST

Syntax

```
delete snmp community="community"
traphost=ipaddress
```

Parameters

community   Specifies the switch's SNMP Read or Write community string. Community strings are 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.

traphost   Specifies the IP address of a management workstation that should not receive traps from the switch.

Description

This command deletes the IP address of a management workstation that you no longer want to receive traps from the switch.

To use this command, you must specify the switch's Read or Write community string. You can specify either string.

To view the community strings and the IP addresses of trap receivers, use the SHOW SNMP command.

Example

The following command deletes the IP address 149.212.11.22 of a management workstation that should no longer receive traps from the switch. It uses the default SNMP Read access community string "public".

```
add snmp community=public traphost=149.212.11.22
```

DESTROY SNMP COMMUNITY

Syntax

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

Parameter

community   Specifies the community string you want to delete from the switch. Community strings are 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 deletes the Read or Write community string from the switch. You must delete a community string prior to assigning a new string. For example, to change the Read community string from its default "public" to something else, you first need to delete the "public" string using this command, and then create the new string using the CREATE SNMP command.

Example

The following command deletes the community string "public":

```
destroy snmp community=public
```

RESET SNMP

Syntax

```
reset snmp
```

Parameters

None.

Description

This command performs the following functions:

❑ Returns the SNMP community strings to the default values, which are "public" for Read access and "private" for Write access.

❑ Disables SNMP access so that the switch cannot be managed using an SNMP application.

❑ Deletes IP addresses of management workstations to receive traps from the switch.

Example

The following command resets SNMP:

```
reset snmp
```

SET SNMP COMMUNITY

Syntax

```
set snmp community="community" access=read|write
```

Parameter

community   Specifies the community string whose access level is to be changed. Community strings are 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.

access   Specifies the new access level for the community string. Options are Read and Write.

Description

This command changes the access level of an existing community string on the switch. For example, you can use the command to change a community string with the Read access level to the Write level. To view the community strings on the switch and their access levels, refer to the SHOW SNMP command.

The switch can support only one community string with the Read access level and one with the Write level at one time. Consequently, in order for you to change a community string's access level, there cannot be on the switch an existing string that was already assigned that level. For instance, to change a community string from the Read to the Write level, you must first delete from the switch the community string that already has been assigned the Write level. To delete community strings, refer to the DESTROY SNMP COMMUNITY command.

Example

The following command changes the access level for the "serv12" community string to Read:

```
set snmp community=serv12 access=read
```

SHOW SNMP

Syntax

```
show snmp
```

Parameters

None.

Description

This command displays the community strings for SNMP Read and Write access on the switch. The default community string for Read access is "public" and the default string for Write access is "private".

This command also displays the IP addresses of management workstations that receive traps from the switch. To add IP address of management stations, refer to the ADD SNMP COMMUNITY TRAPHOST command in this chapter.

Example

The following command displays the SNMP community strings.

```
show snmp
```

Chapter 6

Management Security Commands

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

DISABLE HTTP SERVER

Syntax

```
disable http server
```

Parameters

None.

Description

This command disables the HTTP server on the switch so that the device cannot be managed from a web browser. The default setting is enabled.

Example

The following command disables the HTTP server:

```
disable http server
```

DISABLE SNMP

Syntax

```
disable snmp
```

Parameters

None.

Description

This command disables SNMP on the switch so that the device cannot be managed from a SNMP application program. The default setting is disabled.

Example

The following command disables SNMP:

```
disable snmp
```

ENABLE HTTP SERVER

Syntax

```
enable http server
```

Parameters

None.

Description

This command activates the HTTP server on the switch to allow management of the device from a web browser. The default setting is enabled.

Example

The following command activates the HTTP server:

```
enable http server
```

ENABLE SNMP

Syntax

```
enable snmp
```

Parameters

None.

Description

This command enables SNMP on the switch to permit management of the device from a SNMP application program. The default setting is disabled.

Example

The following command enables SNMP:

```
enable snmp
```

SET PASSWORD MANAGER

Syntax

```
set password manager
```

Parameters

None.

Description

This command sets the manager's password. The default password is "friend". The password can be from 1 to 20 alphanumeric characters. Spaces and special characters, such as exclamation points (!) and asterisks (*), should be avoided. The password is case sensitive.

Example

The following command changes the manager's password:

```
set password manager
```

Follow the prompts to enter the new password.

SET PASSWORD OPERATOR

Syntax

```
set password operator
```

Parameters

None.

Description

This command sets the operator's password. The default password is "operator". The password can be from 1 to 20 alphanumeric characters. Spaces and special characters, such as exclamation points (!) and asterisks (*), should be avoided. 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. The management software automatically ends a management session if it does not detect any activity from the local or remote management station after the specified period of time set by the console timer. This security feature can prevent unauthorized individuals from using your management station should you step away from your system while configuring a switch.

A new console timer takes affect the next time you start a local or remote management session.

Example

The following command sets the console timer to 25 minutes:

```
set switch consoletimer=25
```

SHOW HTTP SERVER

Syntax

```
show http server
```

Parameters

None.

Description

This command displays the status of the HTTP server on the switch. If the status shows enabled, which is the default, you can manage the device from a web browser. If the status shows disabled, the device cannot be managed from a web browser.

Example

The following command displays the status of the HTTP server:

```
show http server
```

Chapter 7

Port Parameter Commands

- ❑ **RESET SWITCH PORT** on page 67

- ❑ **SET SWITCH PORT** on page 68

- ❑ **SHOW SWITCH PORT** on page 73

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

RESET SWITCH PORT

Syntax

```
reset switch port=port
```

Parameter

port   Specifies the port to be reset. You can specify more
                     than one port at a time. You can specify the ports
                     individually (e.g., 2,3,5), as a range (e.g., 7-9), or both
                     (e.g., 2,5,7-9).

Description

This command resets a port. This can prove useful in situations where a
port is experiencing a problem establishing a valid connection to the
end node. The reset takes less than a second to complete. The port's
current parameter settings are not changed by this command. This
command performs the same function as the SOFTRESET option in the
SET SWITCH PORT command.

Example

The following command resets Port 5:

```
reset switch port=5
```

SET SWITCH PORT

Syntax

```
set switch port=port [status=forwarding|disabled]
[description="description"]
[flowcontrol=none|transmit|receive|both]
[backpressure=enable|disable]
[mdimode=mdi|mdix|auto]
[renegotiation=auto]
[softreset=yes|no]
[speed=autonegotiate|10mhalf|10mfull|10mhauto|
10mfauto|100mhalf|100mfull|100mhauto|100mfauto|
1000mfull|1000mfauto|auto10m100m|auto1000m]
[priority=priority] [overridepriority=yes|no]
```

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 (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

status
: Enables or disables a port. You might want to disable a port and prevent it from forwarding packets if a problem occurs with the node or cable connected to the port. Once the problem has been fixed, you can enable the port again to resume normal operation. You can also disable an unused port to secure it from unauthorized connections.

: Possible settings are:

: forwarding
: The port will forward Ethernet frames. This is the default setting for all ports on the switch.

: disabled
: The port will not forward frames.

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.

flowcontrol
: Specifies the flow control on the port. This parameter only applies to ports operating in full-duplex mode. Flow control is used by a port to control the flow of ingress packets. A port uses a special pause packet to stop the end node from

68

sending frames. Possible values for this parameter are:

none	No flow control.
transmit	Flow control when transmitting frames.
receive	Flow control when receiving frames.
both	Flow control when both transmitting and receiving frames.

backpressure
Activates and deactivates backpressure on the port. This parameter only applies to ports operating in half-duplex mode. Backpressure is used by a port to control the flow of ingress packets. A port forces a collision to stop an end node from transmitting data. A collision occurs when two end nodes attempt to transmit data using the same data link at the same time. Values are:

enable	Enables backpressure.
disable	Disables backpressure.

mdimode
Sets the wiring configuration of the port. Possible values are:

mdi	Sets the port's configuration to MDI.
mdix	Sets the port's configuration to MDI-X.
auto	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. This setting is not available if you disable Auto-Negotiation and set the port's speed and duplex settings manually.

renogotiation
Prompts the port to renegotiate speed and duplex mode with the end node. This parameter is only effective when the port is configured for Auto-Negotiation. It can be useful if you believe a port needs to renegotiate speed and duplex mode with the end node. The parameter's one option, AUTO, must always be used with the parameter.

softreset
Resets the port. This option is useful in situations where a port is experiencing a problem establishing a valid connection to the end node. The reset takes less than a second to complete. The port's current

parameter settings are not changed by this command. This parameter performs the same function as the RESET SWITCH PORT command.

speed

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

autonegotiate   The port Auto-Negotiates both speed and duplex mode.This is the default setting.

10mfull   10 Mbps and full-duplex mode.

10mhauto   10 Mbps and half-duplex mode with autonegotiation.

10mfauto   10 Mbps and full-duplex mode with autonegotiation.

100mhalf   100 Mbps and half-duplex mode.

100mfull   100 Mbps and full-duplex mode.

100mhauto   100 Mbps and half-duplex mode with autonegotiation.

100mfauto   100 Mbps and full-duplex mode with autonegotiation.

1000mfull   1000 Mbps and full-duplex mode.

1000mfauto   1000 Mbps and full-duplex mode with autonegotiation.

auto10m100m   This setting is applicable only to the AT-A46 expansion module. It configures the module's 10/100/1000 Mbps port to Auto-Negotiate at 10 or 100 Mbps, full or half duplex mode.

auto1000m   This setting is applicable only to the AT-A46 expansion module. It configures the module's 10/100/1000 Mbps port to Auto-Negotiate at 1000 Mbps only, full or half duplex mode. This is the default setting for an AT-A46 module.

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

priority   Specifies the port's priority. Entering a value of 0 to 3 directs all ingress frames received on the port to the low priority queue on the egress port. Entering a value of 4 to 7 directs all ingress frames to the high priority queue on the egress port. For background information, refer to the description of Class of Service in the **AT-S39 Management Software User's Guide**.

overridepriority Selecting Yes for this parameter causes the port to ignore the tagged header in tagged frames. Tagged frames will be directed to the low or high priority queue on the egress port, depending on the port's priority, set with the PRIORITY option. Specifying No causes the port to determine a frame's priority from its tagged header. The default is No.

Description

This command sets a port's operating parameters.

You should note the following concerning the operation of Auto-Negotiation on a switch port:

❑ In order for a switch port to successfully Auto-Negotiate its duplex mode with an end node, the end node should also be using Auto-Negotiation. Otherwise, a duplex mode mismatch can occur. A switch port using Auto-Negotiation will default to half-duplex if it detects that the end node is not using Auto-Negotiation. This will result in a duplex mismatch if the end node is operating at a fixed duplex mode of full-duplex.

To avoid this problem, when connecting an end node with a fixed duplex mode of full-duplex to a switch port, you should disable Auto-Negotiation on the port and set the port's speed and duplex mode manually.

❑ The auto-MDI/MDI-X setting is available only when a port's speed and duplex mode are set by Auto-Negotiation. If a port's speed or duplex mode is set manually, the port's wiring configuration defaults to MDI-X. Disabling Auto-Negotiation and setting a port's speed and duplex mode manually might require setting the port's MDI/MDI-X setting as well.

Examples

The following command assigns Port 11 the description "Printer port" and configures it to operate at 100 Mbps, half duplex:

```
set switch port=11 description="printer port"
speed=100mhalf
```

The following command sets the wiring configuration for Ports 12 to 16 to MDI-X:

```
set switch port=12-16 mdimode=mdix
```

The following command disables Ports 12 to 16:

```
set switch port=12-16 status=disabled
```

The following command resets Ports 2:

```
set switch port=2 softreset=yes
```

SHOW SWITCH PORT

Syntax

show switch port=*port*

Parameters

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 (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). To view all ports, do not specify a port.

Description

This command displays a port's operating parameters, such as speed and duplex mode.

Examples

The following command displays the operating settings for Port 4:

show switch port=4

The following command displays the operating settings for all ports:

show switch port

Chapter 8

Port Security Commands

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

Note
Refer to the **AT-S39 Management Software User's Guide** for background information on port security.

Note
You can only configure port security from a local management session. You cannot set the feature through enhanced stacking or from a Telnet management session.

SET SWITCH SECURITYMODE

Syntax

```
set switch securitymode=automatic|limited|secure|
locked
```

Parameter

securitymode   Specifies the switch's security mode. Values are:

automatic   Disables port security on the switch. This is the default setting.

limited   Sets the switch to the Limited security mode. This mode allows you to specify a maximum number of MAC addresses each port can learn. To specify a MAC address limit for a port, use the SET SWITCH THRESHOLD command.

secure   Sets the switch to the Secure security mode. In this mode the switch forwards frames based only on static MAC addresses. After activating this security mode, you must enter the static MAC addresses of the nodes with frames the switch is to forward. To add static MAC addresses, use the ADD SWITCH FDB command.

locked   Sets the switch to the Lock All Ports security mode. This mode causes the switch to stop learning new dynamic MAC addresses. The switch forwards frames based on static MAC addresses and on those dynamic addresses it has already learned.

Description

This command sets a switch's port security mode. Only one mode can be active on a switch at a time. To view a switch's current security mode setting, use the SHOW SWITCH command.

Examples

The following command sets the switch's port security mode to limited:

```
set switch securitymode=limited
```

The following command disables port security:

```
set switch securitymode=automatic
```

SET SWITCH THRESHOLD

Syntax

```
set switch threshold=threshold port=port
```

Parameters

threshold   Specifies the maximum number of dynamic MAC addresses a port on the switch can learn. The range is 1 to 150 addresses. The default is 100.

port   Specifies the port whose threshold you want to change. You can specify more than one port at a time. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

Description

This command is used when the switch is operating in the Limited security mode. The Limited security mode allows you to set the maximum number of dynamic MAC addresses the ports on a switch can learn. Once a port has learned its maximum number of MAC addresses, it discards ingress frames with new source MAC addresses.

You can assign different limits to different ports. To view the current threshold levels, use the SHOW SWITCH THRESHOLD command.

Example

The following command sets a threshold limit of 75 dynamic MAC addresses on Ports 5 through 7:

```
set switch threshold=75 port=5-7
```

SHOW SWITCH THRESHOLD

Syntax

```
show switch threshold
```

Parameters

None.

Description

This command displays the threshold limits for all the ports. The threshold limits apply when the switch is operating in the Limited Security Mode. They state the maximum number of dynamic MAC addresses each port can learn. A port that has learned its maximum number of MAC addresses will discard ingress frames from end nodes with MAC addresses not already learned by the port.

Example

The following command displays the threshold limits:

```
show switch threshold
```

Chapter 9
Port Trunking Commands

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

Note
Refer to the **AT-S39 Management Software User's Guide** for guidelines and background information on port trunking.

ADD SWITCH TRUNK

Syntax

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

Parameters

trunk   Specifies the name of the trunk. (You can enter any alphanumeric character for the name and this command will work. This is useful if you have forgotten the name you assigned the trunk.)

port   Specifies the port to be added to the existing port trunk. You can add more than one port. The ports can be specified individually (e.g., 1,2) or as a range (e.g.,1-2). A port trunk cannot have more than four ports.

Description

This command adds one or more ports to an existing port trunk. To view the ports of a trunk, refer to the SHOW SWITCH TRUNK command. To initially create a port trunk, see the CREATE SWITCH TRUNK command.

⚠ **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.

Example

The following command adds Port 5 to the existing port trunk on the switch:

```
add switch trunk=a port=5
```

CREATE SWITCH TRUNK

Syntax

```
create switch trunk=name port=ports
[select=macsrc|macboth]
```

Parameters

trunk   Specifies the name of the trunk. The name can be up to 10 alphanumeric characters. No spaces or special characters are allowed.

port   Specifies the ports of the trunk. A trunk can have up to 4 ports. The ports can be specified individually (e.g., 1,2,5,8), as a range (e.g., 2-5), or both (e.g., 11-13,18).

select   Specifies the load distribution method. Options are:

                     macsrc   Source address (SA) trunking.

                     macboth   Source address / destination address (SA/DA) trunking. This is the default.

Description

This command creates a port trunk. To create the trunk, you specify the ports of the trunk and the load distribution method.

⚠️ **Caution**

Do not connect the cables to the trunk ports on the switches until after you have configured the trunk with 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-S39 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 of Ports 3 through 6 on the switch and assigns it the name "load22." Since no load distribution is specified, MAC source address/destination address is assigned by default:

```
create switch trunk=load22 port=3-6
```

The following command creates a port trunk of Ports 11 through 14 on the switch and assigns it the name "rm44." The load distribution is MAC source address:

```
create switch trunk=rm44 port=11-14 select=macsrc
```

DELETE SWITCH TRUNK

Syntax

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

Parameters

trunk   Specifies the name of the trunk to be modified. (You can enter any alphanumeric character for the name and this command will work. This is useful if you have forgotten the name you assigned the trunk.)

port   Specifies the port to be removed from the existing port trunk. You can remove more than one port at a time. The ports can be specified individually (e.g., 1,4) or as a range (e.g.,1-2).

Description

This command removes ports from an existing port trunk. To view the ports of a trunk, refer to the SHOW SWITCH TRUNK command. To completely remove a port trunk from a switch, see the DESTROY TRUNK command.

⚠ **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 the port trunk:

```
delete switch trunk=a port=9
```

DESTROY SWITCH TRUNK

Syntax

destroy switch trunk=*name*

Parameter

trunk   Specifies the name of the trunk to be deleted. (You can enter any alphanumeric character for the name and this command will still work. This is useful if you forgot the name you assigned the trunk.)

Description

This command deletes the 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 all data cables from the ports of the trunk on the switch before using this command. Deleting 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 deletes the trunk from the switch:

destroy switch trunk=a

SET SWITCH TRUNK

Syntax

```
set switch trunk=name select=macsrc|macboth
```

Parameters

trunk   Specifies the name of the trunk. (You can enter any alphanumeric character for the name and this command will still work. This is extremely useful if you forgot the name you assigned the trunk.)

select   Specifies the load distribution method. Options are:

                macsrc   Source address (SA) trunking.

                macboth   Source address / destination address (SA/DA) trunking. This is the default.

Description

This command changes the load distribution method of the port trunk on the switch. To initially create the port trunk, refer to the CREATE SWITCH TRUNK command. To view the specifics of a trunk, refer to the SHOW SWITCH TRUNK command.

Example

This command changes the load distribution method of the trunk to MAC source address:

```
set switch trunk=a select=macsrc
```

SHOW SWITCH TRUNK

Syntax

```
show switch trunk
```

Parameters

None.

Description

This command displays the ports and the load distribution method of the port trunk.

Example

The following command displays the ports and load distribution method:

```
show switch trunk
```

Chapter 10

Port Mirroring Commands

❑ **ADD SWITCH MIRROR** on page 88

❑ **CREATE SWITCH MIRROR** on page 89

❑ **DELETE SWITCH MIRROR** on page 90

❑ **DESTROY SWITCH MIRROR** on page 91

❑ **SET SWITCH MIRROR** on page 92

❑ **SET SWITCH PORT MIRROR** on page 93

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

Note
For background information on port mirroring, refer to the **AT-S39 Management Software User's Guide**.

ADD SWITCH MIRROR

Syntax

```
add switch mirror srcport=port
```

Parameter

srcports   Specifies the port(s) whose data are to the copied to the destination port. You can specify more than one port. The ports can be specified individually (e.g., 1,2), as a range (e.g., 2-3), or both (1,4,7-9).

Description

This command adds source ports to an existing port mirror. For example, if you were mirroring the traffic on Ports 1 to 4 and you wanted to add port 11 as another source port, you could use this command to add the port to the mirror.

To view the ports of a port mirror, use the SHOW SWITCH command. To initially create a port mirror, refer to the CREATE SWITCH MIRROR command. If you want to change the destination port (that is, the port where the traffic is being copied to), use the SET SWITCH MIRROR command.

Example

The following command adds Port 3 and 4 as additional source ports to an existing port mirror:

```
add switch mirror srcport=3-4
```

CREATE SWITCH MIRROR

Syntax

```
create switch mirror destport=destinationport
srcport=sourceport
```

Parameters

destport   Specifies the destination port where the data will be copied to and where the network analyzer will be connected. You can specify only one destination port.

srcport   Specifies the port whose traffic is to be mirrored. You can specify more that one port. The ports can be specified individually (e.g., 1,4,6), as a range (e.g., 11-14), or both (1,4,7-9).

Description

This command creates a port mirror. To view whether the switch already has a port mirror, use the SHOW SWITCH command.

Examples

The following command creates a port mirror where the traffic on Port 12 (source port) is copied to Port 11 (destination port):

```
create switch mirror destport=11 srcport=12
```

The following command creates a port mirror where the traffic on Ports 1 to 3 (source ports) is copied to Port 4 (destination port):

```
create switch mirror destport=4 srcport=1-3
```

DELETE SWITCH MIRROR

Syntax

```
delete switch mirror srcport=port
```

Parameters

srcports   Specifies the source port(s) to be removed from an existing port mirror. The ports can be specified individually (e.g., 1,2), a range (e.g., 2-3), or both (1,4,7-9).

Description

This command removes a source port(s) from a port mirror. For example, if you are mirroring the traffic on Ports 1 to 4 and you no longer wanted to mirror the traffic on Port 4, you could use this command to remove the port from the mirror.

To view the ports of a port mirror, use the SHOW SWITCH command. To change the destination port (that is, the port where the traffic is being copied to), use the SET SWITCH MIRROR command. To completely delete a port mirror, refer to the DESTROY MIRROR command.

Example

The following command removes Port 9 from a port mirror:

```
delete switch mirror port=9
```

DESTROY SWITCH MIRROR

Syntax

```
destroy switch mirror
```

Parameters

None.

Description

This command deletes a port mirror. Once a port mirror has been deleted, the port that was functioning as the destination (mirror) port can be disconnected from the network analyzer and connected to an end node for normal network operations.

Example

The following command deletes a port mirror:

```
destroy switch mirror
```

SET SWITCH MIRROR

Syntax

```
set switch mirror=port
```

Parameter

mirror   Specifies the new destination port for the mirrored traffic. You can specify only one port.

Description

This command specifies a new destination port of an existing port mirror. The destination port is where the network analyzer is located and where the traffic from the source ports is copied to.

Example

The following command makes Port 11 the new destination port of the port mirror.

```
set switch mirror=11
```

SET SWITCH PORT MIRROR

Syntax

```
set switch port=port mirror=yes|all|no|none
```

Parameters

ports   Specifies the source port(s) to be added or removed from an existing port mirror. The ports can be specified individually (e.g., 1,2), a range (e.g., 2-3), or both (1,4,7-9).

mirror   Specifies whether the source port is to be added or removed. Values are:

           yes, all   Adds the port as a source port to the port mirror. The values are equivalent.

           no, none   Removes the port as a source port from the port mirror. The values are equivalent.

Description

This command adds and removes source ports from an existing port mirror. This command performs the same function as the ADD SWITCH MIRROR command when adding source ports, and the DELETE SWITCH MIRROR command when removing ports.

To initially create a port mirror, refer to the CREATE SWITCH MIRROR command. To view the ports of an existing port mirror, use the SHOW SWITCH command. To change the mirror's destination port (that is, the port where the traffic is being copied to), use the SET SWITCH MIRROR command. To completely delete a port mirror, refer to DESTROY MIRROR.

Examples

The following command adds Port 10 to an existing port mirror:

```
set switch port=10 mirror=yes
```

The following command removes Port 11 from the port mirror:

```
set switch port=11 mirror=no
```

Chapter 11

STP Commands

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

Note
Refer to the **AT-S39 Management Software 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. Once you have selected STP, you can enable or disable it using the ENABLE STP and DISABLE STP commands. A spanning tree protocol is active on a switch only after you designate it as the active spanning tree and enable it.

The default active spanning tree is RSTP. To determine which spanning tree is the currently active spanning tree, use the SHOW SWITCH command.

> **Note**
> Changing the active spanning tree protocol will reboot the switch. Some network traffic may be lost.

When you activate STP, the management software displays a prompt asking if you want to enable the spanning tree. If you select yes, the management software activates STP, resets the switch, and, once the reset process is completed, enables STP. If you select no, the management software activates STP and resets the unit, but does not enable STP. You might select the latter if you want to configure STP parameters before enabling spanning tree.

Example

The following command designates STP as the active spanning tree:

```
activate stp
```

DISABLE STP

Syntax

```
disable stp
```

Parameters

None.

Description

This command disables STP on the switch. The default setting for STP is disabled. To view the current status of STP, use the SHOW STP command.

Example

The following command disables STP:

```
disable stp
```

ENABLE STP

Syntax

```
enable stp
```

Parameters

None.

Description

This command enables STP on the switch. The default setting for STP is disabled. To view the current status of STP, use the SHOW STP command.

Example

The following command enables STP:

```
enable stp
```

RESET STP

Syntax

```
reset 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, use the DISABLE STP command.

Example

The following command returns all STP parameter settings to their default values:

```
reset stp
```

SET STP

Syntax

```
set stp [default] [priority=priority]
[hellotime=hellotime] [forwarddelay=forwarddelay]
[maxage=maxage]
```

Parameters

default   Returns all bridge and port STP settings to the default values. This parameter performs the same function as the RESET STP command. This parameter should not be used with any other command parameter. STP must be disabled in order for you to use this parameter. To disable STP, use the DISABLE 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. When a root bridge goes off-line, the bridge with the next priority number automatically takes over as the root bridge. The range is 0 (zero) to 65,535, with 0 being the highest priority. The default is 32,768.

hellotime   Specifies the time interval between generating and sending configuration messages by the bridge. The range is 1 to 10 seconds. The default is 2 seconds.

forwarddelay   Specifies the waiting period in seconds 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.

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 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 bridge parameters

❑ Bridge priority

❑ Hello time

❑ Forwarding delay

❑ Maximum age time

Examples

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 settings on the switch to the default values:

```
set stp default
```

SET STP PORT

Syntax

```
set stp port=port [default]
[portcost=auto|portcost]
[portpriority=portpriority]
[fastmode=enable|disable][participate=yes|no]
```

Parameters

port   Specifies the port you want to configure. You can specify more than one port at a time. The ports can be specified individually (e.g., 1,2,5,8), as a range (e.g., 2-5), or both (e.g., 11-13,18).

default   Returns the port's STP settings to the default values. This parameter should not be used with any other command parameter. STP must be disabled in order for you to use this parameter. To disable STP, use the DISABLE STP command.

portcost   Specifies the port cost. 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 default value for this parameter is AUTO, which sets port cost according to port speed. The default values are 100 for a 10 Mbps port, 10 for a 100 Mbps port, and 4 for a 1 Gbps port. The range is 1 to 65535.

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 default value for priority is 128. The range is 0 to 255.

fastmode   Specifies a edge port, which is a port that is not connected to another node that is actively running STP. A port where fast mode is enabled skips the STP Listening and Learning states, and goes directly from Blocking to Forwarding. Options for this parameter are:

              enable   Fast mode is enabled. The port skips Listening and Learning states.

              disable   Fast mode is disabled. This is the default setting.

participate Activates and deactivates STP on the port. If you select Yes, which is the default, the port will participate in the spanning tree. If you select No, the port will continue to receive and transmit Ethernet frames, but will not participate in spanning tree.

Note

A port that is not participating in spanning tree is immediately placed in the forwarding state. It cannot be placed in the blocking state by STP should there be a loop in the network topology. Consequently, it is incumbent on the network administrator to insure that no loop will develop should STP be disabled on a port.

Description

This command is used to set the following STP port parameter settings:

❏ Port cost

❏ Port priority

❏ Fast mode

Examples

The following command sets the port cost to 15 and port priority to 100 for Port 6:

```
set stp port=6 portcost=15 portpriority=100
```

The following command activates fast mode on Port 10:

```
set stp port=10 fastmode=enable
```

SHOW STP

Syntax

```
show stp [port=port]
```

Parameters

port   Specifies the port whose STP parameters you want
                    to view. You can specify more than one port at a
                    time. The ports can be specified individually (e.g.,
                    1,2,5,8), as a range (e.g., 2-5), or both (e.g., 11-13,18).

Description

This command displays the STP bridge and port parameter settings.
Values are displayed for the following bridge 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 port
parameters:

❏ 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 12 to 14:

```
show stp port=12-14
```

Chapter 12

RSTP Commands

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

Note
Refer to the **AT-S39 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. A spanning tree protocol is active on a switch only if you designate it as the active spanning tree and enable it.

Note
A change to the active spanning tree protocol will reboot the switch. Some network traffic may be lost.

When you activate RSTP, the management software displays a prompt asking if you want to enable the spanning tree. If you select yes, the management software activates RSTP, resets the switch, and, once the reset process is completed, enables RSTP. If you select no, the management software activates RSTP and resets the unit, but does not enable RSTP. You might select the latter if you want to configure RSTP parameters before enabling spanning tree.

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. The default setting for RSTP is disabled.

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.

Example

The following command enables RSTP:

```
enable rstp
```

RESET RSTP

Syntax

```
reset rstp
```

Parameters

None.

Description

This command returns all bridge and port RSTP parameters to the default settings. RSTP must be disabled in order for you to use this command. To disable RSTP, use the DISABLE RSTP command.

Example

The following command resets RSTP:

```
reset rstp
```

SET RSTP

Syntax

```
set rstp [default] [priority=priority]
[hellotime=hellotime] [forwarddelay=forwarddelay]
[maxage=maxage]
[forceversion=forcestpcompatible|normalrstp]
```

Parameters

default   Disables RSTP and returns all bridge and port RSTP settings to the default values. This option performs the same function as the RESET RSTP command. This parameter should not be used with any other command parameter. RSTP must be disabled in order for you to use this parameter. To disable RSTP, use the DISABLE 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 61440 in increments of 4096. 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 32768 (increment 8).

Table 1 RSTP 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 RSTP 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 default is 15 seconds. This parameter effects only those ports operating in the STP compatible mode.

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. This parameter can be from 6 to 40 seconds. The default is 20 seconds.

Note
The value for the maxage parameter must be less than (2 x (hellotime +1)) and less than (2 x (forwarddelay -1)).

forceversion The forceversion parameter lets you choose between

forcestpcompatible The bridge will use the RSTP parameter settings, but will transmit only STP BPDU packets out the ports.

normalrspt The bridge will use RSTP. This is the default setting.

Description

This command is used to configure the following RSTP parameter settings.

❑ Bridge priority

❑ Hello time

❑ Forwarding delay

❑ Maximum age time

❑ Port priority

❑ Force version of STP or normal RSTP

Examples

The following command returns all RSTP parameter settings to their default values:

```
set rstp default
```

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
set rstp default
```

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=forcestpcompatible
```

SET RSTP PORT

Syntax

```
set rstp port=port [default]
[portcost=auto|portcost]
[portpriority=portpriority][edgeport=yes|no]
[pointtopoint=yes|no|autoupdate]
[migrationcheck=yes|no]
```

Parameters

port
Specifies the port you want to configure. You can specify more than one port at a time. The ports can be specified individually (e.g., 1,2,5,8), as a range (e.g., 2-5), or both (e.g., 11-13,18).

default
Returns the port's RSTP settings to their default values. This parameter should not be used with any other command parameter. RSTP must be disabled in order for you to use this parameter. To disable RSTP, use the DISABLE RSTP command.

portcost
Specifies the port's port cost. 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 range is 0 to 20 000 000. The default setting is AUTO, for Auto-Detect, which automatically sets port cost according to the speed of the port. Table 2 lists the ports cost with Auto-Detect.

Table 2 RSTP Auto-Detect Port Costs

Port Speed	Port Cost
10 Mbps	2 000 000
100 Mbps	200 000
1000 Mbps	20 000

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 of the desired value. The default is 128 (increment 8).

Table 3 RSTP 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. Selections are:

yes   The port is an edge port. This is the default.

no   The port is not an edge port.

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   The port is an point-to-point port.

no   The port is not an point-to-point port.

autoupdate   The port's status is determined automatically. This is the default.

migrationcheck   Instructs the switch to send out RSTP BPDU packets for several seconds from the selected port. The purpose is to determine if there are any RSTP or STP bridges connected to the port. If the port receives STP BPDU packets in response, the port changes to STP compatible mode. If the port receives RSTP BPDU packets, it operates in RSTP.

Description

This command sets a port's RSTP settings.

Examples

The following command sets Port 4's port cost to 1 000 000 and it's port priority to 224:

```
set rstp port=4 portcost=1000000 portpriority=14
```

The following command changes Ports 7 to 10 so they are not considered as edge ports:

```
set rstp port=7-10 edgeport=no
```

The following command returns Port 11 to the default RSTP settings:

```
set rstp port=1 default
```

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 parameter settings for RSTP. Values are displayed for the following parameters:

❑ STP status

❑ Bridge identifier

❑ Bridge priority

❑ Hello time

❑ 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 bridges 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 5:

show rstp portconfig=5

Chapter 13

VLAN Commands

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

Note
For additional information on VLANs, refer to the **AT-S39
Management Software User's Guide**.

ADD VLAN

Syntax 1

```
add vlan=name|vid ports=ports
frame=untagged|tagged [mirrorport=port]
```

Syntax 2

```
add vlan=name|vid taggedports=ports
untaggedports=ports [mirrorport=port]
```

Parameters

vlan   Specifies the name or VID of the VLAN where you want to add tagged or untagged ports.

ports   Specifies the ports to be added to the VLAN. This parameter must be used with the FRAME parameter.

frame   Specifies whether the ports to be added will be tagged or untagged.

taggedports   Specifies the ports on the switch to add as tagged ports to the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

untaggedports   Specifies the ports on the switch that you want to add as untagged ports to the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

mirrorport   Specifies a port on the switch where all traffic on the VLAN will be mirrored. This function is useful in troubleshooting a VLAN. It allows you to mirror the VLAN traffic on another port where you can connect a network analyzer. In most situations you will probably not use this parameter.

Description

This command adds tagged and untagged ports to an existing port-based or tagged VLAN. You can also use this command to mirror the traffic on a VLAN to another port on the switch.

Note
To remove ports from a VLAN, see the command DELETE VLAN.

This command, just like the CREATE VLAN 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 a port as an untagged port to a VLAN, it is automatically removed from its current untagged VLAN assignment. A port can be an untagged member of only one VLAN at a time. For example, adding Port 4 as an untagged port to a VLAN automatically removes it from whichever VLAN where it is an untagged member.

Adding a tagged port to a VLAN does not change the port's current tagged and untagged VLAN assignments. A tagged port can belong to more than one VLAN at a time. For instance, adding Port 6 as an tagged port to a new VLAN does not alter the port's other current 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 name=sales port=4,7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
add vlan name=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 name=production port=3 frame=tagged
```

The following command does the same thing using Syntax 2:

```
add vlan name=production untaggedports=3
```

To add both tagged and untagged ports to a VLAN using Syntax 1 takes two commands. For example, if you had a VLAN called Service and you wanted to add Port 5 as a tagged port and Ports 10 to 12 as untagged ports, the commands would be:

```
add vlan name=Service ports=5 frame=tagged
add vlan name=Service ports=10-12 frame=untagged
```

Using Syntax 2, you can do the whole thing with just one command:

```
add vlan name=Service untaggedports=10-12
taggedports=5
```

CREATE VLAN

Syntax 1

```
create vlan=name vid=vid ports=ports|all
frame=untagged|tagged [mirrorport=port]
```

Syntax 2

```
create vlan=name vid=vid taggedports=ports|all
untaggedports=ports|all [mirrorport=port]
```

Parameters

vlan   Specifies the name of the VLAN. A VLAN must be assigned a name.

                     The name can be from one to ten characters in length. The name 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 will be unique in your network, then the name should be unique as well. If the VLAN will be part of a larger VLAN that spans multiple switches, then the name for the VLAN should be the same on each switch where nodes of the VLAN are connected.

vid   Specifies the VLAN identifier. The range is 2 to 4094. The VLAN must be assigned a VID.

                     You cannot use the VID 1; that value 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 will be unique in your network, then its VID must also be unique. If this VLAN will be 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 will span three switches, you should assign the Sales VLAN on each switch the same VID value.

ports	Specifies the ports on the switch that are to be either tagged or untagged members of the new VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). 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 PORTS parameter.
taggedports	Specifies the ports on the switch to serve as tagged ports in the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). To specify all ports on the switch, use ALL. Omit this parameter if the VLAN will not contain tagged ports.
untaggedports	Ports on the switch to function as untagged ports in the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). To specify all ports on the switch, use ALL. Omit this parameter if the VLAN will not contain untagged ports.
MirrorPort	A port on the switch where all traffic on the VLAN will be mirrored. This function is useful in troubleshooting a VLAN. It allows you to mirror the VLAN traffic on another port where you can connect a network analyzer. The mirror port can be a member of the same VLAN it will be used to monitor or a member of another VLAN. In most situations you will probably not use this parameter.

Description

This command creates a port-based or tagged VLAN.

As shown at the start of this section, this command features two syntaxes. You can use either syntax to create a port-based or tagged VLAN. The difference between the two is how you go about specifying which ports are to be members of the VLAN and whether the ports will be tagged or untagged. Syntax 1 is limited in that it allows you to specify either tagged or untagged ports, but not both in the same command. Syntax 2, on the other hand, can create a VLAN that has both types of ports with one command. This is illustrated in the section **Examples** 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 where 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 an tagged port to a new VLAN, Port 6 remains a member of any current VLAN assignments as untagged and tagged members.

Examples

The following command uses Syntax 1 to create a port-based VLAN called Sales with a VID of 3 and untagged ports 4-9 and 14:

```
create vlan name=Sales vid=3 ports=4-9,14
frame=untagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan name=Sales vid=3 untaggedports=4-9,14
```

The following command uses Syntax 1 to create a tagged VLAN called Production with a VID of 22 and tagged ports 3 and 6:

```
create vlan name=Production vid=22 ports=3,6
frame=tagged
```

The following command uses Syntax 2 to create the same VLAN:

```
create vlan name=Sales vid=22 taggedports=3,6
```

Now let's try creating an tagged VLAN that contains both untagged and tagged ports. 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 14. You could not create this VLAN using Syntax 1 with just one command. It would actually take two commands. You would first create the VLAN, specifying either the untagged or tagged ports. For example:

```
create vlan name=Service vid=16 ports=1,4,5-7
frame=untagged
```

Then, to add the other ports to the VLAN (in this case tagged ports), you would use the ADD VLAN command.

Syntax 2 can create a VLAN of both tagged and untagged ports all in one command. Here is the command that would create our example:

```
create vlan name=Service vid=16
untaggedports=1,4,5-7 taggedports=11,14
```

That's the advantage of Syntax 2 over Syntax 1. You can create VLANs containing both types of ports in one command rather than two commands.

DELETE VLAN

Syntax 1

```
delete vlan=name|vid ports=ports|all
frame=untagged|tagged [mirrorport=port]
```

Syntax 2

```
delete vlan=name|vid taggedports=ports|all
untaggedports=ports|all [mirrorport=port]
```

Parameters

vlan	Specifies the name or VID of the VLAN from which ports are to be removed.
ports	Specifies the ports to be removed from the VLAN. This parameter must be used with the FRAME parameter.
frame	Specifies whether the ports to be removed are tagged or untagged.
taggedports	Specifies the tagged ports on the switch that you want to remove from the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). Specifying ALL removes all tagged ports from the VLAN.
untaggedports	Specifies the untagged ports on the switch that you want to remove from the VLAN. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9). Specifying ALL removes all untagged ports from the VLAN.
mirrorport	Specifies the port on the switch which is to stop functioning as a mirror port of the VLAN.

Description

This command removes tagged and untagged ports from a VLAN. You can also use this command to cancel a port functioning as a VLAN mirror.

This command has two syntaxes, just like the CREATE VLAN command. 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 **Examples** below.

123

Note
To delete a VLAN, see the command DESTROY VLAN.

Note
You cannot change the name or VID of a VLAN.

When an untagged port is deleted from a VLAN, it is automatically returned to the Default_VLAN as an untagged member. If a port is also functioning as a tagged member of other VLANs, it remains a 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 a tagged port is removed 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 name=sales port=4,7 frame=untagged
```

The following command does the same thing using Syntax 2:

```
delete vlan name=sales untaggedports=4,7
```

The following command uses Syntax 1 to delete tagged Port 3 from a VLAN called Production:

```
delete vlan name=production port=3 frame=tagged
```

The following command does the same thing using Syntax 2:

```
delete vlan name=production untaggedports=3
```

To delete both tagged and untagged ports from a VLAN using Syntax 1 takes two commands. For example, if you had a VLAN called Service and you wanted to delete tagged Port 5 and untagged Ports 10 to 12, the commands would be:

```
delete vlan name=Service ports=5 frame=tagged
delete vlan name=Service ports=10-12
frame=untagged
```

Using Syntax 2, you can do the whole thing with just one command:

```
delete vlan name=Service untaggedports=10-12
taggedports=5
```

DESTROY VLAN

Syntax

```
destroy vlan=name
```

Parameter

vlan   Specifies the name of the VLAN to be deleted.

Description

This command deletes port-based and tagged VLANs from a switch. All untagged ports in a deleted VLAN are automatically returned to the Default_VLAN.

You cannot delete the Default_VLAN.

Examples

The following command deletes the VLAN Sales from the switch:

```
destroy vlan=sales
```

RESET VLAN

Syntax

```
reset vlan
```

Parameters

Description

This command deletes all port-based and tagged VLANs on a switch, except for the Default_VLAN. All ports are returned to the Default_VLAN as untagged ports. To delete individual VLANs, refer to the DESTROY VLAN command.

Example

The following command deletes VLANs on a switch:

```
reset vlan
```

SET SWITCH INFILTERING

Syntax

```
set switch infiltering=on|off
```

Parameter

infiltering   Specifies the status of ingress filtering. Options are:

        on   Ingress filtering is activated.

        off   Ingress filtering is deactivated.

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.

Example

The following command deactivates ingress filtering:

```
set switch infiltering=off
```

SET SWITCH MANAGEMENTVLAN

Syntax

```
set switch managementvlan=name|vid
```

Parameters

managementvlan   Specifies the management VLAN. You can specify the VLAN by name or VID. You can specify only one management VLAN. The VLAN must already exist on the switch. 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 remote Telnet and web browser management sessions. For background information on the function of the management VLAN, refer to the **AT-S39 Management Software 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 SWITCHMODE

Syntax

```
set switch switchmode=tagged|basic
```

Parameters

vlanmode   Specifies the switch's mode. Specifying TAGGED
                    means the switch will support user-configured (port-
                    based and tagged) and multiple (801.Q compliant and
                    non-801.Q compliant) VLANs. Specifying BASIC means
                    the switch will support the Basic switch mode. The
                    default is tagged. Only one mode can be active on a
                    switch at a time.

Description

This command configures a switch to support port-based and tagged
VLANs or the Basic mode.

Example

The following command configures the switch to support the Basic
mode:

```
set switch switchmode=basic
```

SET SWITCH VLANMODE

Syntax

```
set switch vlanmode=userconfig|multiple|
dotqmultiple
```

Parameters

vlanmode   Specifies the switch's VLAN mode. Options are:

USERCONFIG   Sets the switch to support port-based and tagged VLANs. This is the default.

MULTIPLE   Configures the switch for the non-801.Q compliant multiple VLANs mode.

DOTQMULTIPLE   Configures the switch for the 801.Q compliant multiple VLANs mode. The default is USERCONFIG.

Description

This command configures the switch's VLAN Mode. The mode can be user-configured, which supports port-based and tagged VLANs, or one of two multiple VLAN modes.

Note
The switch can only support these VLAN modes when its mode is set to tagged. To set the switch mode, refer to the SET SWITCH SWITCHMODE command.

Example

The following command configures the switch to support 801.Q compliant VLAN mode:

```
set switch vlanmode=dotqmultiple
```

SET SWITCH VLANSTATUS

Syntax

```
set switch vlanstatus=enable|disable
```

Parameters

vlanstatus   Specifies the switch's mode. Specifying ENABLE
                    means the switch will support user-configured (port-
                    based and tagged) and multiple (801.Q compliant and
                    non-801.Q compliant) VLANs. Specifying DISABLE
                    means the switch will support the Basic switch mode.
                    The default is tagged and untagged VLANs. Only one
                    mode can be active on a switch at a time.

Description

This command configures a switch to support tagged VLAN switch
mode or the Basic switch mode.

> **Note**
> This command performs the same function as the SET SWITCH
> SWITCHMODE command.

Example

The following command configures the switch to support the Basic
switch mode:

```
set switch vlanstatus=disable
```

SHOW VLAN

Syntax

```
show vlan[=name|vid]
```

Parameters

vlan   Specifies the name or VID of the VLAN.

Description

This command displays all the port-based and tagged VLANs on a switch. The information includes the names of the VLANs, the VIDs, and the port members.

Examples

The following command displays all the VLANs on the switch:

```
show vlan
```

The following command displays information on the Sales VLAN:

```
show vlan=sales
```

Chapter 14
MAC Address Table Commands

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

ADD SWITCH FDB

Syntax

```
add switch fdb macaddress=macaddress port=port
```

Parameters

macaddress   Specifies the static unicast or multicast address to add to the switch's MAC address table. The address can be entered in either of the following formats:

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

port   Specifies the port to which the MAC address is to be assigned. For a unicast address, you can specify only one port. For a multicast address, you can specify multiple ports.

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.

Examples

The following command adds the static MAC address 00:A0:D2:18:1A:11 to Port 7:

```
add switch fdb macaddress=00A0D2181A11 port=7
```

The following command adds the multicast MAC address 01:00:51:00:00 10 to Ports 9 and 10:

```
add switch fdb macaddress=010051000010 port=9-10
```

DELETE SWITCH FDB

Syntax

```
delete switch fdb macaddress=macaddress
[vlan=name|VID]
```

Parameters

address   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 where the address was learned or assigned. The VLAN can be specified by name or VID. This parameter is optional when deleting a unicast address and mandatory for a multicast address.

Description

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

Examples

The following command deletes the unicast MAC address 00:A0:D2:18:1A:11 from the table:

```
delete switch fdb macaddress=00A0D2181A11
```

The following command deletes the multicast MAC address 01:00:51:00:00:11 from the table. The switch ports where the address was assigned belong to the Sales VLAN:

```
delete switch fdb macaddress=010051000011
vlan=sales
```

SET SWITCH AGINGTIMER

Syntax

```
set switch agingtimer=value
```

Parameter

agingtimer   Specifies the aging timer for the MAC address table. The value is in seconds. The range is 1 to 1048575. The default is 300 seconds (5 minutes).

Description

The switch uses the aging time 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.

Example

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

```
set switch agingtimer=120
```

SHOW SWITCH FDB

Syntax

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

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 the dynamic and static unicast addresses learned or assigned to a particular port on the switch. You can specify only one port.

status   Specifies the type of MAC addresses you want to view. Choices are:

         static   Displays static unicast and multicast addresses.

         dynamic   Displays dynamic unicast and multicast addresses.

         multicast   Displays dynamic multicast addresses.

vlan   Specifies a VLAN. Use this parameter to view the static and dynamic unicast and multicast addresses learned or assigned to the ports of a particular VLAN on the switch. The VLAN can be identified by name or VID.

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

Description

This command displays the dynamic and static unicast and multicast MAC addresses stored in a switch's MAC address table. The information includes the following:

MAC
The unicast or multicast MAC address.

Port
The port on the switch where the unicast MAC address was learned or assigned. This column is empty for a multicast address.

PMAP
The ports on the switch that are members of a multicast group. This column is useful in determining which ports belong to different multicast groups. (The abbreviation PMAP is derived from "port mapping.")

Each "0" is a hexadecimal value for the binary value "0000". Each binary "0" represents a port on the switch. A binary "0" means that the port is not a member of a multicast group while a "1" means that it is.

The port numbering scheme is from right to left. As an example, assume that ports 1 through 4 on the switch were members of the same multicast group. This would be represented in the column as follows: "0000000F". Another example is "000020F. This example would indicate that ports 1 to 4 and port 10 on the switch were members of the same multicast group.

This column is empty for unicast addresses.

CPU
This feature is not supported.

MIR
Indicates whether the traffic on the port is being mirrored. Yes means the traffic is being mirrored while No indicates that it is not.

EMP
Indicates whether multicast packets are being forwarded by ports in the blocking state. This feature is not supported at this time. This column will indicate "No" for all multicast addresses, except for the switch's MAC address. Multicast packets are forwarded only by ports in the forwarding state.

VLANID
The VID of the VLAN to which the port is an untagged member.

Type
The MAC address type. The type can be either static or dynamic.

Examples

The following command displays all MAC addresses in the switch's MAC address table:

```
show switch fdb
```

The following command displays just the multicast addresses:

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

The following command displays the port number 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 dynamic MAC addresses learned on Port 11:

```
show switch fdb port=11
```

The following command displays the MAC addresses learned on the ports in the Sales VLAN:

```
show switch fdb vlan=sales
```

Chapter 15
IGMP Snooping Commands

❑ **SET IP IGMP** on page 142

❑ **SHOW IP IGMP** on page 144

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

Note
For background information on IGMP snooping, refer to the **AT-S39 Management Software User's Guide**.

SET IP IGMP

Syntax

```
set ip igmp [snoopingstatus=enable|disable]
[hoststatus=singlehost|multihost]
[timeout=timeout] [numbermulticastgroups=number]
[routerport=portnumber|auto]
```

Parameters

snoopingstatus   Activates and deactivates IGMP snooping on the switch. Possible settings are:

     enable   Activates IGMP snooping.

     disable   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 reports 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 will learn. This parameter is useful with networks that contain a large number of multicast groups. You can use the parameter to prevent the switch's MAC address table

from filling up with multicast addresses, leaving no room for dynamic or static MAC addresses. The range is 1 to 2048 addresses. The default is 256 addresses.

routerport   Specifies the port(s) on the switch connected to a multicast router. Specifying AUTO activates auto-detect, where the switch automatically determines the ports with multicast routers. Auto-detect is the default setting.

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=enable
hoststatus=multihost timeout=120
```

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.

routerlist   Displays the ports on the switch that are connected to multicast routers.

Description

Displays the IGMP parameter settings. This command can also display a list of host nodes as well as a list of switch ports connected to multicast routers.

Note
For instructions on how to set the IGMP parameters, refer to the SET IGMP command.

Examples

The following command displays the current IGMP parameter settings:

```
show ip igmp
```

The following command displays a list of host nodes:

```
show ip igmp hostlist
```

Chapter 16
Broadcast Frame Control Command

❑ **SET SWITCH BROADCAST** on page 146

❑ **SET SWITCH PORT BCLIMIT** on page 148

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

Note
For background information on broadcast frame control, refer to the **AT-S39 Management Software User's Guide**.

SET SWITCH BROADCAST

Syntax

```
set switch broadcast timer10_100mbps=integer
timer1000mbps=integer
```

Parameters

timer10_100mbps Specifies the broadcast timer interval for ports operating at 10 Mbps or 100 Mbps. The range is 10 to 120 milliseconds, in increments of 10, with a default of 10 milliseconds.

timer1000mbps Specifies the length of time, in microseconds, for ports operating at 1000 Mbps. The range is 100 to 12,000 microseconds, in increments of 100, with a default of 100 microseconds.

Description

This command specifies the broadcast interval timer which defines the time period used in counting the number of forwarded egress broadcast frames on a port. There are two interval timers. One timer is for ports operating at 10 Mbps and 100 Mbps. The second timer is for 1000 Mbps ports. The timer interval for 10 and 100 Mbps ports is measured in milliseconds. The timer interval for 1000 Mbps ports is measured in microseconds. A time interval setting applies to all ports operating at the corresponding speed on the switch.

> **Note**
> The 1000 Mbps speed applies only to optional Gigabit Ethernet ports.

Both timers round down your input. For the timer interval for 10 and 100 Mbps ports, values you enter are rounded down to the nearest multiple of 10. For the 1000 Mbps timer, values you enter are rounded down to the nearest multiple of 100 microseconds.

To set the maximum number of broadcast frames a port will transmit, refer to the SET SWITCH PORT BCLIMIT command.

Examples

The following command sets a broadcast timer of 500 milliseconds for ports operating at 10 Mbps or 100 Mbps:

```
set switch broadcast timer10_100mbps=500
```

146

The following command sets a broadcast timer of 200 microseconds for ports operating at 1000 Mbps:

```
set switch broadcast timer1000mbps=200
```

SET SWITCH PORT BCLIMIT

Syntax

```
set switch port=port bclimit=broadcastlimit
```

Parameters

port   Specifies the port where you want to configure the broadcast limit. You can specify more than one port at a time. You can specify the ports individually (e.g., 2,3,5), as a range (e.g., 7-9), or both (e.g., 2,5,7-9).

bclimit   Specifies the maximum number of broadcast frames the port will transmit during the interval specified by the broadcast timer. The range is 0 to 1023. The default is "0", which disables frame control on the port.

Description

This command specifies the maximum number of egress broadcast frames the port will transmit during the interval specified by the broadcast timer. Egress broadcast frames over the maximum number are discarded by the port.

To view the broadcast frame limits on the ports, use the SHOW SWITCH PORT command. To set the broadcast timer, refer to the SET SWITCH BROADCAST command.

Examples

This command sets the broadcast limit on port 4 to 100 egress broadcast packets:

```
set switch port=5 bclimit=100
```

This command disables the broadcast limit on ports 7 and 12:

```
set switch port=7,12 bclimit=0
```

Chapter 17

TACACS+ and RADIUS Commands

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

Note
For background information on TACACS+ and RADIUS authentication protocols, refer to the **AT-S39 Management Software User's Guide**.

ADD RADIUSSERVER

Syntax

```
add radiusserver ipaddress=ipaddress
order=integer [secret=string] [port=integer]
```

Parameters

ipaddress   Specifies an IP address of a RADIUS server.

order   Specifies the order that your RADIUS server is queried by the switch. You can assign order to up to 3 servers with 1 being the first server queried.

secret   Specifies the encryption key used for this server.

port   Specifies the UDP (User Datagram Protocol) port of the RADIUS server.

Description

Use this command to specify the IP address of a RADIUS server and the order it is queried by the switch. You may specify an encryption key and a UDP port.

Examples

The following command adds a RADIUS server with the 149.245.22.22 IP address and specifies it is the first server in the list.

```
add radiusserver ipaddress=149.245.22.22 order=1
```

The following command adds the RADIUS server with the 149.245.22.22 IP address. In addition, it specifies your server is the third RADIUS server to be queried by the switch and it has a UDP port of 3.

```
add radiusserver ipaddress=149.245.22.22 order=2
port=3
```

The following command adds a RADIUS server with an IP address of 149.245.22.22. In addition, it specifies the order is 2, the encryption key is tiger74, and the UDP port is 1.

```
add radiusserver ipaddress=149.245.22.22 order=2
secret=tiger74 port=1
```

ADD TACACSSERVER

Syntax

```
add tacacsserver ipaddress=ipaddress
order=integer [secret=string]
```

Parameters

ipaddress   Specifies an IP address of a TACACS+ server.

order   Specifies the order that your TACACS+ server is 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 address of a TACACS+ server to your
switch along with order the TACACS+ server is 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 lioness54 as the encryption code.

```
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 and specifies that this TACACS+ server is the third
TACACS+ server queried by the switch.

```
add tacacsserver ipaddress=149.245.22.26 order=3
```

DELETE RADIUSSERVER

Syntax

```
delete radiusserver ipaddress=ipaddress
```

Parameters

ipaddress   Specifies the IP address of your RADIUS server to be deleted.

Description

Use this command to delete a RADIUS server with the specified IP address 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 ipaddress=ipaddress
```

Parameters

ipaddress   Specifies the IP address of the TACACS+ server that you want to delete.

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 of 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. This command does not effect 802.1x port-based access control. Disabling authentication means that you must use the default manager accounts of "manager" and "operator" to manage the switch.

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. To select an authenticator protocol, refer to **SET AUTHENTICATION** on page 157.

Note
This command applies only to TACACS+ and RADIUS manager accounts. This command does not effect 802.1x port-based access control. If you are using the RADIUS authentication protocol for 802.1x port-based access control, but not for manager account authentication, you do not need to enable authentication. You can leave the RADIUS manager account feature disabled and the switch will still have access to the RADIUS configuration information for 802.1x port-based access control.

Example

The following command enables manager account authentication on the switch:

```
enable authentication
```

RESET AUTHENTICATION

Syntax

```
reset authentication
```

Parameter

None.

Description

This command performs nearly the same function as the DISABLE AUTHENTICATION command. It disables authentication and, additionally, returns the authentication method to TACACS+. The current authentication settings are retained, including server IP addresses and encryption keys (both local and global).

Example

The following command resets authentication on the switch:

```
reset authentication
```

SET AUTHENTICATION

Syntax

```
set authentication method=[tacacs|radius]
[secret=string] [timeout=integer]
```

Parameter

method   Specify either the TACACS+ or RADIUS protocol to run on your switch.

secret   Specify the global encryption key that is used for all of your TACACS+ or RADIUS servers. If the servers use different encryption keys, you can leave this parameter blank and set individual encryption keys with the ADD TACACSSERVER or ADD RADIUSSERVER commands.

timeout   Specifies the maximum amount of time the switch waits for a response from either the TACACS+ or RADIUS server before the switch assumes the server cannot 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 or if there isn't a list of servers, the switch defaults to the standard Manager and Operator accounts. The default is 30 seconds. The range is 1 to 300 seconds.

Description

Use this command to select the authentication protocol. You may specify a global encryption code and the maximum number of seconds the switch waits for a response from either the TACACS+ or RADIUS server.

Examples

The following command selects TACACS+ as the authentication protocol on your switch:

```
set authentication method=tacacs
```

The following command selects TACACS+ as the authentication protocol with 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

Parameters

None.

Description

Use this command to display the following information about the authenticated protocols on the switch:

❑ The status of your authenticated protocol: enabled or disabled.

❑ The authentication protocol activated on your switch. Either TACACS+ or RADIUS protocols may be active. The TACACS+ protocol is the default.

❑ The IP addresses of up to 3 authentication servers.

❑ The encryption key for each individual server, if defined.

❑ The global encryption code that applies to all authentication servers.

❑ The length of the time, in seconds, before the switch assumes the server cannot respond.

Example

The following command displays authentication protocol information on your switch:

show authentication

Chapter 18

802.1x Port-Based Access Control Commands

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

Note
You must use a local management session to configure port-based access control. You cannot configure this feature through enhanced stacking or from a Telnet management session.

Note
For background information on 802.1x port-based access control, refer to the **AT-S39 Management Software User's Guide**.

DISABLE PORTACCESS

Syntax

```
disable portaccess
```

Parameters

None.

Description

This command disables 802.1x port-based access control on the switch. When disabled, supplicant end nodes can pass traffic through the switch without logging on. The default settings for 802.1x port-based access is disabled.

> **Note**
> This command must be performed from a local management session.

Example

The following command disables port-based access control on your switch:

```
disable portaccess
```

ENABLE PORTACCESS

Syntax

```
enable portaccess
```

Parameters

None.

Description

Use this command to enable 802.1x port-based access control on your switch. When enabled, supplicant nodes must log on to pass traffic through the switch.

> **Note**
> You should configure the RADIUS client software on the switch before enabling port-based access control. Refer to **SET AUTHENTICATION** on page 157.

> **Note**
> This command must be performed from a local management session.

Example

The following command enables 802.1x port-based access control on the switch:

```
enable portaccess
```

SET PORTACCESS

Syntax

```
set portaccess port=port
[role=none|authenticator]
[control=auto|forceauthenticate|
forceunauthenticate]
[quietperiod=integer] [txperiod=integer]
[reauthperiod=integer] [supptimeout=integer]
[servtimeout=integer] [maxreq=integer]
```

Parameters

port Specifies the port whose port-based access control role or settings you want to change. You can specify more than one port at a time.

role Specifies the role of the port. The role can be one of the following:

   authenticator Specifies the Authenticator role.

   none Disables port-based access control on the port. This is the default setting.

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.
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.
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.
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.

servtimeout This is the timer used by the switch to determine authentication server timeout conditions. The default value for this parameter is 30 seconds. The range is 1 to 65,535 seconds.

maxreq This parameter 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 default value for this parameter is 2 retransmissions. The range is 1 to 10 retransmissions.

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.

Note
This command must be performed from a local management session.

Examples

This command sets port 1 to the authenticator role:

```
set portaccess port=1 role=authenticator
```

This command sets ports 5 and 10 to the Authenticator role and sets the servertimeout parameter to 200 seconds:

```
set portaccess ports=5,10 role=authenticator
servtimeout=200
```

This command disables 802.1x port-based access control on ports 7 to 12:

```
set portaccess ports=7-12 role=none
```

SHOW PORTACCESS

Syntax

```
show portaccess config|status
```

Parameters

config   Displays the port-based access control roles and settings for all ports.

status   Displays the status and role of the ports. You can use this parameter only when port-based access is enabled.

Description

This command displays 802.1x port-based access control configuration and status information on the switch ports.

Example

The following command displays port parameter settings for the port-based access control feature:

```
show portaccess config
```

Chapter 19

Statistics Commands

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

RESET SWITCH COUNTER

Syntax

```
reset switch counter
```

Parameters

None.

Description

This command returns all statistics counters on the switch to zero (0).

Example

The following command resets the statistics counters:

```
reset switch counter
```

RESET SWITCH PORT COUNTER

Syntax

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

Parameters

port   Specifies the port whose statistics counter you want to
               return to zero. You can specify more than one port at a
               time. The ports can be specified individually (e.g.,
               1,2,5,8), as a range (e.g., 2-5), or both (e.g., 11-13,18).

Description

This command returns the statistics counters for a port to zero.

Example

The following command returns the counters on Ports 4 and 5 to zero.

```
reset switch port=4,5 counter
```

SHOW SWITCH COUNTER

Syntax

```
show switch counter
```

Parameters

None.

Description

This command displays switch operating statistics, such as the number of packets received and transmitted, and the number of CRC errors. For definitions of the statistics, refer to the **AT-S39 User's Guide**.

Example

The following command displays switch operating statistics:

```
show switch counter
```

SHOW SWITCH PORT COUNTER

Syntax

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

Parameters

port   Specifies the port whose statistics you want to view. You can view more than one port at a time. The ports can be specified individually (e.g., 1,2,5,8), as a range (e.g., 2-5), or both (e.g., 11-13,18). 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 definitions of the statistics, refer to the **AT-S39 Management Software User's Guide**.

Examples

The following command displays the operating statistics for Port 4:

```
show switch port=4 counter
```

The following command displays the operating statistics for all ports:

```
show switch port counter
```

Chapter 20
Download and Upload Commands

❏ **LOAD** on page 173

❏ **UPLOAD** on page 178

Note
For background information on downloading and uploading software images and configuration files, refer to the **AT-S39 User's Guide**.

LOAD

Syntax

```
load method=tftp|xmodem|remoteswitch
type=image|config|bootloader
switchnumber=switches
```

Parameters

method
: Specifies the method of the download. Options are:

  tftp
  : Indicates that the download will use TFTP. This download method can be used from either a local or remote management session.

  xmodem
  : Indicates that the download will use Xmodem. This download method can be used from a local management session only.

  remoteswitch
  : Indicates that the download will be from a master switch to other switches in an enhanced stack. This option must be used from a master switch and together with the SWITCHNUMBER option.

type
: Specifies the file to be downloaded. Options are:

  image
  : Downloads both the AT-S39 software image and bootloader.

  config
  : Downloads a configuration file.

  bootloader
  : Downloads just the bootloader.

  You can specify only one file type at a time.

switchnumber
: Specifies the switch in an enhanced stack to which you want to download a new version of AT-S39 software or configuration file. This option, which must be used with the METHOD=REMOTESWITCH option, instructs the master switch to download its AT-S39 software or configuration file onto the specified switch. Switch numbers are displayed with the SHOW REMOTELIST command. You can specify more than one switch at a time (e.g., 1,3,4).

Description

This command can download a new version of the AT-S39 software image file or switch configuration onto an AT-8000 Series switch. You can use this command to download files as follows:

❑ From a local management session

❑ From a remote management session

❑ From a master switch to other switches in an enhanced stack

To download a file locally, you must start a local management session directly on the switch. This entails connecting a terminal or PC with a terminal emulator program to the RS232 Terminal Port on the switch, as explained in the **AT-S39 Management Software User's Guide**. You can use either Xmodem, or if the switch has an IP address and subnet mask, TFTP.

You can also download a file to a remote switch. This can be a switch accessed through enhanced stacking or from a Telnet management session. This type of download uses TFTP exclusively. For this type of download, the switch must have an IP address and subnet mask.

The final method is switch-to-switch. Here, you instruct the master switch of an enhanced stack to download its AT-S39 image file or configuration file to other switches in the enhanced stack. This method is useful if you have a large number of AT-8000 Series switches in your network. You can download the AT-S39 software from the master switch to the other switches in an enhanced stack so that all the switches are using the same version of management software.

With a switch-to-switch download, you can also download the master switch's configuration file to other switches. This is useful in network environments where there are a AT-8000 Series switches that need to be configured the same, or nearly the same. You can configure the master switch of an enhanced stack network, and then download its configuration file to the other switches, saving you the trouble of having to configure each switch individually.

Here are general guidelines that apply to all download methods:

❑ All switch models in the AT-8000 Series use the same AT-S39 software image.

❑ In networks consisting of several AT-8000 switches, you can simplify an upgrade procedure by upgrading a master switch to the latest software version via a local or Telnet management session and then downloading the new software switch-to-switch from the master switch to the slave switches.

❑ The image file and bootloader were offered as two separate files in several earlier software versions. In this version, the two files are combined into one file.

❑ It is not recommended that you download the bootloader by itself. If the bootloader on a switch needs to be updated, you should download the entire AT-S39 software image.

❑ If you are downloading a new AT-S39 software image, the switch's current settings (for instance, IP address, port security, and virtual LANs) are not changed.

❑ If you are downloading a configuration file, the current configuration of the switch is overwritten by the configuration contained in the file.

❑ A configuration file contains all switch settings, including the IP address, subnet mask, gateway address, enhanced stacking status, and BOOTP/DHCP status.

❑ A configuration file should only be downloaded onto a switch of the same model from which the configuration file originated (for example, AT-8024M to AT-8024M). It is not recommended that you download a configuration file onto a switch of a different model (for example, AT-8012M to AT-8024GB). The results can be unpredictable.

❑ A switch running AT-S39 Version 1.4 or earlier must first be ungraded to Version 1.4.1 or 1.4.2 before you can install a new AT-S39 image.

❑ A configuration file cannot be edited with a text editor or word processor.

⚠ **Caution**
Downloading a new AT-S39 image file or configuration file will cause a switch reset. Some network traffic may be lost.

Here are guidelines that apply to an Xmodem download:

❑ Xmodem can only download a file onto the switch where you started the local management session. Xmodem cannot download files through enhanced stacking.

❑ The file to be downloaded must be stored on the computer or terminal connected to the RS232 Terminal Port on the switch.

Here are guidelines that apply to a TFTP download:

❑ There must be a node on your network that contains the TFTP server software. The AT-S39 image file or configuration file to be downloaded must be stored on the server.

❑ You should start the TFTP server before you begin the download procedure.

❑ The switch on which you are downloading the file must have an IP address and subnet mask, such as a master switch of an enhanced stack. You cannot use TFTP on a slave switch, since that type of switch typically does not have an IP address. Instead, you would need to perform the download from a local management session of the switch using Xmodem or, alternatively switch to switch using the REMOTESWITCH parameter.

Here is a guideline that applies to a switch-to-switch download:

❑ You must always use the SHOW REMOTELIST command first to determine the switch numbers. (This also allows the management software to determine the number and type of switches in the enhanced stack.)

⚠ **Caution**
If you are downloading an AT-S39 image file, the switch must initialize the software once it has received the file. The initialization process that can take several minutes to complete. Do not interrupt the initialization process by resetting or power cycling the switch. Once the initialization process is complete, the switch resets.

Xmodem Examples

The following command downloads a new AT-S39 software image from the management workstation to the switch:

```
load method=xmodem type=image
```

After you have entered the command, the management software will display a confirmation prompt followed by another prompt instructing you to begin the file transfer. To begin the transfer, use your terminal emulation program to specify the location of the AT-S39 software image file stored on your workstation that you want to download onto the switch.

The following command downloads a new AT-S39 configuration from the management workstation to the switch:

```
load method=xmodem type=config
```

After entering this command, you must specify the location of the AT-S39 configuration file stored on your workstation using your terminal emulation program.

TFTP Examples

The following command downloads the AT-S39 image file using TFTP:

```
load method=tftp type=image
```

You are prompted for the IP address of the TFTP server and the name of the image file to download.

The following command downloads a configuration file:

```
load method=tftp type=config
```

Again, you are prompted for the IP address of the TFTP server and the name of the file to download.

Switch-to-switch Examples

The following command downloads the AT-S39 image file on the master switch to switches 1 and 4 in an enhanced stack. (Switch numbers are displayed using the SHOW REMOTELIST command.)

```
load method=remoteswitch type=image
switchnumber=1,4
```

The following command downloads the AT-S39 configuration file on the master switch to switch 2 in an enhanced stack.

```
load method=remoteswitch type=config
switchnumber=2
```

UPLOAD

Syntax

upload method=tftp|xmodem type=image|config

Parameters

method   Specifies the method of the upload. Options are:

                 tftp   Indicates that the upload will be performed using TFTP. This upload method can be used from either a local or remote management session.

                 xmodem   Indicates that the upload method will be Xmodem. This upload method can be used from a local management session only.

type   Specifies the file to be uploaded. Options are:

                 image   Uploads both the AT-S39 software image and bootloader.

                 config   Uploads the switch's configuration file.

                 You can specify only one file at a time.

Description

This command uploads the AT-S39 software image and bootloader from a switch to a management workstation.

This command can also upload a switch's configuration file to a management workstation. You might upload a configuration file so that you can download it onto another switch. This is useful in network environments where there are AT-8000 Series switches that need to be configured the same, or nearly the same. You can configure one switch, upload its configuration file to a management workstation, and then download it to the other switches, saving you the trouble of having to configure each switch individually.

You can upload files as follows:

❏   From a local management session

❑ From a remote management session

To upload a file locally, you must start a local management session directly on the switch. This involves connecting a terminal or PC with a terminal emulator program to the RS232 Terminal Port on the switch, as explained in the **AT-S39 Management Software User's Guide**. You can use either Xmodem, or if the switch has an IP address and subnet mask, TFTP.

You can also upload a file from a remote switch. This can be a switch accessed through enhanced stacking or from a Telnet management session. This type of download uses TFTP exclusively and requires that the switch have an IP address and subnet mask.

Here are general guidelines that apply to all upload methods:

❑ A configuration file contains all switch settings, including the IP address, subnet mask, gateway address, enhanced stacking status, and BOOTP/DHCP status.

❑ You cannot edit a configuration file with a text editor or word processor.

Note
It is not recommended that you upload an AT-S39 software image onto a management workstation for download onto another switch. New AT-S39 software images for download onto a switch should be obtained from the Allied Telesyn web site.

Here is a guideline that applies to Xmodem uploads:

❑ Xmodem can only upload a file from the switch where you started the local management session. Xmodem cannot upload files through enhanced stacking.

Here are guidelines that apply to a TFTP upload:

❑ There must be a node on your network that contains the TFTP server software.

❑ You should start the TFTP server before you begin the download procedure.

❑ The switch from where you are uploading the file must have an IP address and subnet mask.

Xmodem Examples

The following command uploads the switch's configuration file to the management workstation:

```
upload method=xmodem type=config
```

After entering the command, use your terminal emulator program to indicate where you want to store the file on your workstation and the filename.

The following command uploads the switch's AT-S39 image to the management workstation:

```
upload method=xmodem type=image
```

TFTP Example

The following command uploads a switch's configuration file using TFTP:

```
upload method=tftp type=config
```

You are prompted for the IP address of the TFTP server.

Chapter 21
Command Reference

Basic Command Line Commands

CLEAR SCREEN

```
clear screen
```

Clears the screen.

HELP

```
help
```

Displays a list of command keywords.

LOGOFF and QUIT

```
logoff
quit
```

Ends a management session.

MENU

```
menu
```

Displays the AT-S39 Main Menu.

SAVE CONFIGURATION

```
save configuration
```

Saves your changes to the switch's flash memory for permanent storage.

SET PROMPT

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

Sets the command line prompt.

SET SWITCH CONSOLEMODE

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

Specifies whether management sessions are to start with the command line interface or the menu interface.

SHOW USER

```
show user
```

Displays your manager account username.

Basic Switch Commands

DISABLE DHCPBOOTP

```
disable dhcpbootp
```

Deactivates the DHCP and BOOTP client software on the switch.

ENABLE DHCPBOOTP

```
enable dhcpbootp
```

Activates the DHCP and BOOTP client software on the switch.

PING

```
ping ipaddress
```

Instructs the switch to ping an end node.

PURGE IP

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

Returns a switch's IP address, subnet mask, or default gateway address to its default value.

RESET IP

```
reset ip interface=1
```

Returns a switch's IP address, subnet mask, and gateway address to the default values.

RESET SYSTEM

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

Deletes a switch's name, the name of the network administrator responsible for managing the unit, and the location of the unit.

RESTART REBOOT

```
restart reboot
```

Returns the switch's operating parameters to the default settings.

RESTART SWITCH

```
restart switch
```

Resets the switch.

SET IP

```
set ip interface=1 ipaddress=IPaddress|DHCP
netmask=subnetmask
```

Configures the switch's IP address and subnet mask, or activates the DHCP and BOOTP client software.

SET IP ROUTE

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

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

SET SYSTEM

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

Sets a switch's name, the name of the network administrator responsible for managing the unit, and the location of the unit.

SHOW CONFIG

```
show config
```

Displays overall information on the switch and the ports.

SHOW DHCPBOOTP

```
show dhcpbootp
```

Displays the status of the DHCP and BOOTP client software on the switch.

SHOW IP

```
show ip interface=1
```

Displays the IP address, subnet mask, and default gateway.

SHOW IP ROUTE

```
show ip route
```

Displays the switch's default gateway address.

SHOW SWITCH

```
show switch
```

Displays a variety of switch information, including the MAC aging time, console timer, broadcast timers, and VLAN mode.

SHOW SYSTEM

```
show system
```

Displays the AT-S39 software version and build date, bootloader version and build date, serial number, model name, switch name, name of the network administrator responsible for managing the unit, and location of the unit.

Enhanced Stacking Commands

ACCESS SWITCH

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

Start a management session on another switch in an enhanced stack.

EXIT

```
exit
```

Ends a management session and returns you back to the master switch from which you started the session or, if you enter this command from a master switch, exits you from the command line prompt and displays the AT-S39 Main Menu.

SET SWITCH STACKMODE

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

Sets a switch's enhanced stacking status.

SHOW REMOTELIST

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

Displays a lists of the switches of an enhanced stack.

SNMP Community Strings and Trap Commands

ADD SNMP COMMUNITY TRAPHOST

`add snmp community="`*`community`*`" traphost=`*`ipaddress`*

Adds to a community string the IP address of a management workstation to receive management traps from the switch.

CREATE SNMP COMMUNITY

`create snmp community="`*`community`*`"`
`access=read|write [traphost=`*`ipaddress`*`]`

Creates a new Read or Write community string on the switch.

DELETE SNMP COMMUNITY TRAPHOST

`delete snmp community="`*`community`*`"`
`traphost=`*`ipaddress`*

Deletes the IP address of a management workstation that is not to receive traps from the switch.

DESTROY SNMP COMMUNITY

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

Deletes the Read or Write community string from the switch.

RESET SNMP

`reset snmp`

Returns the SNMP community strings to the default values, disables SNMP access, and deletes the IP addresses of trap receivers.

SET SNMP COMMUNITY

`set snmp community="`*`community`*`" access=read|write`

Changes the access level of an existing community string on the switch.

SHOW SNMP

`show snmp`

Displays the SNMP community strings.

Management Security Commands

DISABLE HTTP SERVER

```
disable http server
```

Disables the HTTP server on the switch so that the device cannot be managed from a web browser.

DISABLE SNMP

```
disable snmp
```

Disables SNMP on the switch so that the device cannot be managed from a SNMP application program.

ENABLE HTTP SERVER

```
enable http server
```

Enables the HTTP server on the switch so that the device can be managed from a web browser.

ENABLE SNMP

```
enable snmp
```

Enables SNMP on the switch so that the device can be managed from a SNMP application program.

SET PASSWORD MANAGER

```
set password manager
```

Sets the manager's password.

SET PASSWORD OPERATOR

```
set password operator
```

Sets the operator's password.

SET SWITCH CONSOLETIMER

```
set switch consoletimer=value
```

Sets the console timer.

SHOW HTTP SERVER

```
show http server
```

Displays the status of the HTTP server on the switch.

Port Parameter Commands

RESET SWITCH PORT

```
reset switch port=port
```

Resets a port.

SET SWITCH PORT

```
set switch port=port [status=forwarding|disabled]
[description="description"]
[flowcontrol=none|transmit|receive|both]
[backpressure=enable|disable]
[mdimode=mdi|mdix|auto]
[renegotiation=auto]
[softreset=yes|no]
[speed=autonegotiate|10mhalf|10mfull|10mhauto|
10mfauto|100mhalf|100mfull|100mhauto|100mfauto|
1000mfull|1000mfauto|auto10m100m|auto1000m]
[priority=priority] [overridepriority=yes|no]
```

Sets a port's operating parameters. (You can set only one parameter at a time with this command.)

SHOW SWITCH PORT

```
show switch port=port
```

Displays a port's operating parameters, such as speed and duplex mode.

Port Security Commands

SET SWITCH SECURITYMODE

```
set switch securitymode=automatic|limited|secure|
locked
```

Sets a switch's port security mode.

SET SWITCH THRESHOLD

```
set switch threshold=threshold port=ports
```

Sets the maximum number of dynamic MAC addresses a port can learn when the switch is operating in the Limited security mode.

SHOW SWITCH THRESHOLD

```
show switch threshold
```

Displays the threshold limit for each port when the switch is operating in the Limited security mode.

Port Trunking Commands

ADD SWITCH TRUNK

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

Add ports to an existing port trunk.

CREATE SWITCH TRUNK

```
create switch trunk=name port=ports
[select=macsrc|macboth]
```

Creates a port trunk.

DELETE SWITCH TRUNK

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

Removes ports from a port trunk.

DESTROY SWITCH TRUNK

```
destroy switch trunk=name
```

Deletes a port trunk from the switch.

SET SWITCH TRUNK

```
set switch trunk=name select=macsrc|macboth
```

Changes the load distribution method of a port trunk.

SHOW SWITCH TRUNK

```
show switch trunk
```

Displays the ports of a port trunk and the load distribution method.

Port Mirroring Commands

ADD SWITCH MIRROR

```
add switch mirror srcport=port
```

Adds a source port(s) to an existing port mirror.

CREATE SWITCH MIRROR

```
create switch mirror destport=destinationport
srcport=sourceport
```

Creates a port mirror.

DELETE SWITCH MIRROR

```
delete switch mirror srcport=port
```

Removes a source port(s) from a port mirror.

DESTROY SWITCH MIRROR

```
destroy switch mirror
```

Deletes a port mirror, making it possible to connect the destination (mirror) port to an end node for normal network operations.

SET SWITCH MIRROR

```
set switch mirror=port
```

Specifies a new destination port of an existing port mirror.

SET SWITCH PORT MIRROR

```
set switch port=port mirror=yes|all|no|none
```

Adds and deletes source ports from a port mirror.

Spanning Tree Protocol Commands

ACTIVATE STP

```
activate stp
```

Designates STP as the active spanning tree.

DISABLE STP

```
disable stp
```

Disables STP on the switch.

ENABLE STP

```
enable stp
```

Enables STP on the switch.

RESET STP

```
reset stp
```

Returns all STP bridge and port parameters to the default settings.

SET STP

```
set stp [default] [priority=priority]
[hellotime=hellotime] [forwarddelay=forwarddelay]
[maxage=maxage]
```

Sets the STP bridge parameter settings.

SET STP PORT

```
set stp port=port [default]
[portcost=auto|portcost]
[portpriority=portpriority]
[fastmode=enable|disable][participate=yes|no]
```

Sets the STP port parameter settings.

SHOW STP

```
show stp [port=port]
```

Displays the STP parameter settings.

Rapid Reconfiguration Spanning Tree Commands

ACTIVATE RSTP

```
activate rstp
```

Designates RSTP as the active spanning tree on the switch.

DISABLE RSTP

```
disable rstp
```

Disables RSTP on the switch.

ENABLE RSTP

```
enable rstp
```

Enables RSTP on the switch.

RESET RSTP

```
reset rstp
```

Returns all bridge and port RSTP parameters to the default settings.

SET RSTP

```
set rstp [default] [priority=priority]
[hellotime=hellotime] [forwarddelay=forwarddelay]
[maxage=maxage]
[forceversion=forcestpcompatible|normalrstp]
```

Sets the RSTP parameter settings.

SET RSTP PORT

```
set rstp port=port [default]
[portcost=auto|portcost]
[portpriority=portpriority] [edgeport=yes|no]
[pointtopoint=yes|no|autoupdate]
[migrationcheck=yes|no]
```

Sets a port's RSTP parameter settings.

SHOW RSTP

```
show rstp [portconfig=port|portstate=port]
```

Displays the RSTP parameter settings.

VLAN Commands

ADD VLAN

Syntax 1

```
add vlan=name|vid ports=ports
frame=untagged|tagged [mirrorport=port]
```

Syntax 2

```
add vlan=name|vid taggedports=ports
untaggedports=ports [mirrorport=port]
```

Adds tagged and untagged ports to existing port-based and tagged VLANs.

CREATE VLAN

Syntax 1

```
create vlan=name vid=vid ports=ports|all
frame=untagged|tagged [mirrorport=port]
```

Syntax 2

```
create vlan=name vid=vid taggedports=ports|all
untaggedports=ports|all [mirrorport=port]
```

Creates port-based and tagged VLANs.

DELETE VLAN

Syntax 1

```
delete vlan=name|vid ports=ports
frame=untagged|tagged [mirrorport=port]
```

Syntax 2

```
delete vlan=name|=vid taggedports=ports
untaggedports=ports [mirrorport=port]
```

Removes tagged and untagged ports from port-based and tagged VLANs.

DESTROY VLAN

```
destroy vlan=name
```

Deletes port-based and tagged VLANs.

RESET VLAN

`reset vlan`

Deletes all port-based and tagged VLANs, except for the Default_VLAN.

SET SWITCH INFILTERING

`set switch infiltering=on|off`

Activates and deactivates ingress filtering.

SET SWITCH MANAGEMENTVLAN

`set switch managementvlan=name|vid`

Sets the switch's management VLAN, used for remote Telnet and web browser management.

SET SWITCH SWITCHMODE

`set switch switchmode=tagged|basic`

Configures a switch to support either port-based and tagged VLANs or the Basic mode.

SET SWITCH VLANMODE

`set switch vlanmode=userconfig|multiple|`
`dotqmultiple`

Configures the switch to support port-based and tagged VLANs or one of the multiple VLAN modes.

SET SWITCH VLANSTATUS

`set switch vlanstatus=enable|disable`

Configures a switch to support either port-based and tagged VLANs or the Basic mode.

SHOW VLAN

`show vlan[=name|vid]`

Displays the VLANs on the switch.

MAC Address Table Commands

ADD SWITCH FDB

```
add switch fdb macaddress=macaddress port=port
```

Adds static unicast and multicast MAC addresses to the switch's MAC address table.

DELETE SWITCH FDB

```
delete switch fdb macaddress=macaddress
[vlan=name|VID]
```

Deletes dynamic and static unicast and multicast addresses from the switch's MAC address table.

SET SWITCH AGINGTIMER

```
set switch agingtimer=value
```

Sets the aging timer for the MAC address table.

SHOW SWITCH FDB

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

Displays the dynamic and static unicast and multicast MAC addresses stored in a switch's MAC address table.

IGMP Snooping Commands

SET IP IGMP

```
set ip igmp [snoopingstatus=enable|disable]
[hoststatus=singlehost|multihost]
[timeout=timeout] [numbermulticastgroups=number]
[routerport=portnumber|auto]
```

Configures the IGMP snooping parameters.

SHOW IP IGMP

```
show ip igmp [hostlist|routerlist]
```

Displays the IGMP parameter settings, host nodes, and multicast router ports.

Broadcast Frame Control Commands

SET SWITCH BROADCAST

```
set switch broadcast timer10_100mbps=integer
timer1000mbps=integer
```

Specifies the broadcast interval timers.

SET SWITCH PORT BCLIMIT

```
set switch port=port bclimit=broadcastlimit
```

Specifies the maximum number of egress broadcast frames the port will transmit during the interval specified by the broadcast timer.

TACACS+ and RADIUS Commands

ADD RADIUSSERVER

```
add radiusserver ipaddress=ipaddress
order=integer [secret=string] [port=integer]
```

Adds the IP address of a RADIUS server to the switch.

ADD TACACSSERVER

```
add tacacsserver ipaddress=ipaddress
order=integer [secret=string]
```

Adds the IP address of a TACACS+ server to the switch.

DELETE RADIUSSERVER

```
delete radiusserver ipaddress=ipaddress
```

Deletes the IP address of a RADIUS server from the switch.

DELETE TACACSSERVER

```
delete tacacsserver ipaddress=ipaddress
```

Deletes the IP address of a TACACS+ server from the switch.

DISABLE AUTHENTICATON

```
disable authentication
```

Disables TACACS+ and RADIUS management account authentication on the switch.

ENABLE AUTHENTICATON

```
enable authentication
```

Enables TACACS+ and RADIUS management account authentication on the switch.

RESET AUTHENTICATON

```
reset authentication
```

Disables TACACS+ and RADIUS authentication.

SET AUTHENTICATON

```
set authentication method=[tacacs|radius]
[secret=string] [timeout=integer]
```

Selects the authentication protocol.

SHOW AUTHENTICATON

```
show authentication
```

Displays information about the authenticated protocols on the switch.

802.1x Port-Based Access Network Control

DISABLE PORTACCESS

```
disable portaccess
```

Disables port-based access control on the switch.

ENABLE PORTACCESS

```
enable portaccess
```

Enables port-based access control on the switch.

SET PORTACCESS

```
set portaccess port=port
[role=none|authenticator]
[control=auto|forceauthenticate|
forceunauthenticate] [quietperiod=integer]
[txperiod=integer] [reauthperiod=integer]
[supptimeout=integer] [servtimeout=integer]
[maxreq=integer]
```

Sets port-based access control parameters.

SHOW PORTACCESS STATUS

`show portaccess status`

Displays the port-based access control status on the switch.

Statistics Commands

RESET SWITCH COUNTER

`reset switch counter`

Returns all statistics counters on the switch to zero (0).

RESET SWITCH PORT COUNTER

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

Returns the statistics counters for a port to zero.

SHOW SWITCH COUNTER

`show switch counter`

Displays a switch's operating statistics, such as the number of packets received and transmitted, and the number of CRC errors.

SHOW SWITCH PORT COUNTER

`show switch port[=`*`port`*`] counter`

Displays the operating statistics for a port on the switch.

Download and Upload Commands

LOAD

```
load method=tftp|xmodem|remoteswitch
type=image|config|bootloader
switchnumber=switches
```

Downloads a new version of the AT-S39 software image or a configuration file onto an AT-8000 Series switch.

UPLOAD

```
upload method=tftp|xmodem type=image|config
```

Uploads the AT-S39 software image or configuration file from a switch to a management workstation or tftp server.

Index