CHAPTER 4

Configuring System Management Functions

This chapter describes the basic tasks for configuring general system features, such as access control and basic switch management.

Note This chapter provides advanced configuration instructions for the Catalyst 8540 MSR, Catalyst 8510 MSR, and LightStream 1010 ATM switch routers. For complete descriptions of the commands mentioned in this chapter, refer to the *ATM Switch Router Command Reference* publication.

The following sections describe basic tasks for configuring general system features, such as access control and basic switch management tasks:

System Management Tasks

The role of the administration interface is to provide a simple command-line interface to all internal management and debugging facilities of the ATM switch router.

Configuring Terminal Lines and Modem Support (Catalyst 8540 MSR)

The Catalyst 8540 MSR has a console terminal line that might require configuration. For line configuration, you must first set up the line for the terminal or the asynchronous device attached to it. For a complete description of configuration tasks and commands used to set up your terminal line and settings, refer to the *Dial Solutions Configuration Guide* and *Dial Solutions Command Reference* publications.

You can connect a modem to the console port. The following settings on the modem are required:

- Enable auto answer mode
- Suppress result codes

You can configure your modem by setting the dual in-line package (DIP) switches on the modem or by connecting the modem to terminal equipment. Refer to the user manual provided with your modem for the correct configuration information.

Note Because there are no hardware flow control signals available on the console port, the console port terminal characteristics should match the modem settings.

Configuring Terminal Lines and Modem Support (Catalyst 8510 MSR and LightStream 1010)

The Catalyst 8510 MSR and LightStream 1010 ATM switch routers have two types of terminal lines: a console line and an auxiliary line. For line configuration, you must first set up the lines for the terminals or other asynchronous devices attached to them. For a complete description of configuration tasks and commands used to set up your lines, modems, and terminal settings, refer to the *Dial Solutions Configuration Guide* and *Dial Solutions Command Reference* publications.

Configuring Alias

You can create aliases for commonly used or complex commands. Use word substitutions or abbreviations to tailor command syntax. For detailed instructions on performing these tasks, refer to the *Configuration Fundamentals Configuration Guide* publication.

Configuring Buffers

To make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed, use the following global configuration command:

Command	Purpose
buffers {**small** | **middle** | **big** | **verybig** | **large** | **huge** | *type number*}	Configures buffers; the default huge buffer size is 18024 bytes.
show buffers [**all** | **assigned** [**dump**]]	Displays statistics for the buffer pools on the network server.

To display the buffer pool statistics, use the following privileged EXEC command:

Command	Purpose
show buffers [**address** *hex-addr* | **all** | **assigned** | **free** | **input-interface** *type card/subcard/port* | **old** | **pool** *name* [**dump** | **header** | **packet**]] [**failures**]	Displays statistics for the buffer pools on the network server.

Configuring Cisco Discovery Protocol

To specify how often your ATM switch router sends Cisco Discovery Protocol (CDP) updates, perform the following tasks in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **cdp holdtime** *seconds*	Specifies the hold time in seconds, to be sent in packets.
Step 2	Switch(config)# **cdp timer** *seconds*	Specifies how often your ATM switch router will send CDP updates.
Step 3	Switch(config)# **cdp run**	Enables CDP.

To reset CDP traffic counters to zero (0) on your ATM switch router, perform the following tasks in privileged EXEC mode:

	Command	Purpose
Step 1	Switch# **clear cdp counters**	Clears CDP counters.
Step 2	Switch# **clear cdp table**	Clears CDP tables.

To show the CDP configuration, use the following privileged EXEC commands:

Command	Purpose
show cdp	Displays global CDP information.
show cdp *entry-name* [**protocol** | **version**]	Displays information about a neighbor device listed in the CDP table.
show cdp interface [*interface-type interface-number*]	Displays interfaces on with CDP enabled.
show cdp neighbors [*interface-type interface-number*] [**detail**]	Displays CDP neighbor information.
show cdp traffic	Displays CDP traffic information.

Configuring Enable Passwords

To log on to the ATM switch router at a specified level, use the following EXEC command:

Command	Purpose
enable *level*	Enables login.

To configure the enable password for a given level, use the following global configuration command:

Command	Purpose
enable password [**level** *number*] [*encryption-type*] *password*	Configures the enable password.

Configuring Load Statistics Interval

To change the length of time for which data is used to compute load statistics, perform the following tasks, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface** {**atm** | **ethernet**} **0** Switch(config-if)#	Selects the route processor interface to be configured.
Step 2	Switch(config-if)# **load-interval** *seconds*	Configures the load interval.

Configuring Logging

To log messages to a syslog server host, use the following global configuration commands:

Command	Purpose
logging *host*	Configures the logging name or IP address of the host to be used as a syslog server.
logging buffered [*level* | *size*]	Logs messages to an internal buffer, use the **logging buffered** global configuration command. The **no logging buffered** command cancels the use of the buffer and writes messages to the console terminal, which is the default.
logging console *level*	Limits messages logged to the console based on severity, use the **logging console** global configuration command.
logging facility *type*	Configures the syslog facility in which error messages are sent, use the **logging facility** global configuration command. To revert to the default of local, use the **no logging facility** global configuration command.

Command	Purpose
logging monitor *level*	Limits messages logged to the terminal lines (monitors) based on severity, use the **logging monitor** global configuration command. This command limits the logging messages displayed on terminal lines other than the console line to messages with a level at or above *level.* The **no logging monitor** command disables logging to terminal lines other than the console line.
logging on	Controls logging of error messages, use the **logging on** global configuration command. This command enables or disables message logging to all destinations except the console terminal. The **no logging on** command enables logging to the console terminal only.
logging trap *level*	Limits messages logged to the syslog servers based on severity, use the **logging trap** global configuration command. The command limits the logging of error messages sent to syslog servers to only those messages at the specified level. The **no logging trap** command disables logging to syslog servers.
logging source-interface *type identifier*	Specifies the interface for source address in logging transactions.

Configuring Login Authentication

To enable TACACS+ authentication for logins, perform the following steps, beginning in global configuration mode:

Command	Purpose
line [**aux** | **console** | **vty**] *line-number* [*ending-line-number*]	Selects the line to configure.
login [**local** | **tacacs**]	Configures login authentication.

Configuring Scheduler Attributes

To control the maximum amount of time that can elapse without running the lowest-priority system processes, use the following global configuration commands:

Command	Purpose
scheduler allocate *msecs*	Configures the guaranteed CPU time for processes, in milliseconds. The minimum interval is 500 ms; the maximum value is 6000 ms.
scheduler process-watchdog {**hang** | **normal** | **reload** | **terminate**}	Configures scheduler process-watchdog action for looping processes.
scheduler interval *msecs*	Specifies maximum time in milliseconds that can elapse without running system processes.

Configuring Services

To configure miscellaneous system services, use the following global configuration commands:

Command	Purpose
service alignment	Configures alignment correction and logging.
service compress-config	Compresses the configuration file.
service config	Loads config TFTP files.
service disable-ip-fast-frag	Disables IP particle-based fast fragmentation.
service exec-callback	Enables EXEC callback.
service exec-wait	Configures a delay of the start-up of the EXEC on noisy lines.
service finger	Allows Finger protocol requests (defined in RFC 742) from the network server.
service hide-telnet-addresses	Hides destination addresses in Telnet command.
service linenumber	Enables a line number banner for each EXEC.
service nagle	Enables the Nagle congestion control algorithm.
service old-slip-prompts	Allows old scripts to operate with SLIP/PPP.
service pad	Enables Packet Assembler Dissembler commands.
service password-encryption	Enables encrypt passwords.
service prompt	Enables a mode-specific prompt.
service slave-log	Enables log capability on slave IPs.
service tcp-keepalives {**in** | **out**}	Configures keepalive packets on idle network connections.
service tcp-small-servers	Enables small TCP servers (for example, ECHO).

Command	Purpose
service telnet-zero-idle	Sets the TCP window to zero (0) when the Telnet connection is idle.
service timestamps	Displays timestamp debug/log messages.
service udp-small-servers	Enables small UDP servers (for example, ECHO).

Configuring SNMP

To create or update an access policy, use the following global configuration commands:

Command	Purpose
snmp-server access-policy *destination-party source-party context privileges*	Configures global access policy.
snmp-server chassis-id *text*	Provides a message line identifying the SNMP server serial number.
snmp-server community *string* [**RO** | **RW**] [*number*]	Configures the SNMP community access string.
snmp-server contact *text*	Configures the system contact (syscontact) string.
snmp-server context *context-name context-oid view-name*	Configures a context record.
snmp-server enable	Enables SNMP traps or informs.
snmp-server host *name community-string* [**envmon**] [**frame-relay**] [**sdlc**] [**snmp**] [**tty**] [**x25**]	Configures the recipient of an SNMP trap operation.
snmp-server location *text*	Configures a system location string.
snmp-server packetsize *byte-count*	Configures the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.
snmp-server party *party-name party-oid* [*protocol-address*] [**packetsize** *size*] [**local** | **remote**] [**authentication** {**md5** *key* [**clock** *clock*] [**lifetime** *lifetime*] | **snmpv1** *string*}]	Configures a party record.
snmp-server queue-length *length*	Configures the message queue length for each trap host.
snmp-server system-shutdown	Enables use of the SNMP reload command.
snmp-server trap-authentication [**snmpv1** | **snmpv2**]	Configures trap message authentication.
snmp-server trap-timeout *seconds*	Configures how often to resend trap messages on the retransmission queue.
snmp-server view *view-name mib-tree* {**included** | **excluded**}	Configures view entry.

To display the SNMP status, use the following EXEC command:

Command	Purpose
show snmp	Checks the status of communications between the SNMP agent and SNMP manager.

Username Commands

To establish a username-based authentication system at login, use the following global configuration commands:

Command	Purpose
username *name* [**dnis**] [**nopassword** | **password** [*encryption-type*] *password*]	Configures username-based authentication system at login.
username *name* **password** *secret*	Configures username-based CHAP authentication system at login.
username *name* **autocommand** *command*	Configures username-based authentication system at login with an additional command to be added.
username *name* **nohangup**	Configures username-based authentication system at login and prevents Cisco IOS from disconnecting after the automatic command is completed.
username *name* **noescape**	Configures username-based authentication system at login but prevents the user from issuing an escape character on the switch.
username *name* **privilege** *level*	Sets user privilege level.

Configuring the Privilege Level

This section describes configuring and displaying the privilege level access to the ATM switch router. The access privileges can be configured at the global level or at the line level for a specific line.

Configuring Privilege Level (Global)

To set the privilege level for a command, use the following global configuration command:

Command	Purpose
privilege *mode* **level** *number command* [*type*]	Sets the privilege level.

To display your current level of privilege, use the following privileged EXEC command:

Command	Purpose
show privilege	Displays the privilege level.

Configuring Privilege Level (Line)

To set the default privilege level for a line, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **line** [**aux** | **console** | **vty**] *line-number* [*ending-line-number*]	Selects the line to configure.
Step 2	Switch(config-line)# **privilege level** *number*	Configures the default privilege level.

To display your current level of privilege, use the following privileged EXEC command:

Command	Purpose
show privilege	Displays the privilege level.

Configuring the Network Time Protocol

This section describes configuring the Network Time Protocol (NTP) on the ATM switch router.

To control access to the system NTP services, use the following **ntp** global configuration commands. To remove access control to the system's NTP services, use the **no ntp** command. See the example configuration at the end of this section and the "Displaying the NTP Configuration" section on page 4-12 to confirm the NTP configuration.

To see a list of the NTP commands enter a **?** in EXEC configuration mode. The following example shows the list of commands available for NTP configuration:

```
Switch(config)# ntp ?
  access-group        Control NTP access
  authenticate        Authenticate time sources
  authentication-key  Authentication key for trusted time sources
  broadcastdelay      Estimated round-trip delay
  clock-period        Length of hardware clock tick
  master              Act as NTP master clock
  max-associations    Set maximum number of associations
  peer                Configure NTP peer
  server              Configure NTP server
  source              Configure interface for source address
  trusted-key         Key numbers for trusted time sources
  update-calendar     Periodically update calendar with NTP time
```

To control access to the system NTP services, use the following global configuration command:

Command	Purpose
ntp access-group {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*	Configures an NTP access group.

To enable NTP authentication, perform the following steps in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **ntp authenticate**	Enables NTP authentication.
Step 2	Switch(config)# **ntp authentication-key** *number* **md5** *value*	Defines an authentication key.

To specify that a specific interface should send NTP broadcast packets, perform the following steps, beginning to global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface** *type card/subcard/port* Switch(config-if)#	Selects the physical interface to be configured.
Step 2	Switch(config-if)# **ntp broadcast** [**client** | **destination** | **key** | **version**]	Configures the system to receive NTP broadcast packets.

As NTP compensates for the error in the system clock, it keeps track of the correction factor for this error. The system automatically saves this value into the system configuration using the **ntp clock-period** global configuration command.

Caution Do not enter the **ntp clock-period** command; it is documented for informational purposes only. The system automatically generates this command as NTP determines the clock error and compensates.

To prevent an interface from receiving NTP packets, perform the following steps, beginning in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **interface** *type card/subcard/port* Switch(config-if)#	Selects the physical interface to be configured.
Step 2	Switch(config-if)# **ntp disable**	Disables the NTP receive interface.

To configure the ATM switch router as a NTP master clock to which peers synchronize themselves when an external NTP source is not available, use the following global configuration command:

Command	Purpose
ntp master [*stratum*]	Configures NTP master clock.

To configure the ATM switch router as a NTP peer that receives its clock synchronization from an external NTP source, use the following global configuration command:

Command	Purpose
ntp peer *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	Configures the system clock to synchronize a peer or to be synchronized by a peer.

To allow the ATM switch router system clock to be synchronized by a time server, use the following global configuration command:

Command	Purpose
ntp server *ip-address* [**version** *number*] [**key** *keyid*] [**source** *interface*] [**prefer**]	Configures the system clock to allow it to be synchronized by a time server.

To use a particular source address in NTP packets, use the following global configuration command:

Command	Purpose
ntp source *interface type card/subcard/port*	Configures a particular source address in NTP packets.

To authenticate the identity of a system to which NTP will synchronize, use the following global configuration command:

Command	Purpose
ntp trusted-key *key-number*	Configures an NTP synchronize number.

To periodically update the ATM switch router calendar from NTP, use the following global configuration command:

Command	Purpose
ntp update-calendar	Updates an NTP calendar.

Example

The following example configures the ATM switch router to synchronize its clock and calendar to an NTP server, using ethernet0, and other features:

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ntp server 198.92.30.32
Switch(config)# ntp source ethernet0
Switch(config)# ntp authenticate
Switch(config)# ntp max-associations 2000
Switch(config)# ntp trusted-key 22507
Switch(config)# ntp update-calendar
```

Displaying the NTP Configuration

To show the status of NTP associations, use the following privileged EXEC commands:

Command	Purpose
show ntp associations [**detail**]	Displays NTP associations.
show ntp status	Displays the NTP status.

Examples

The following example displays detail NTP configuration:

```
Switch# show ntp associations detail
198.92.30.32 configured, our_master, sane, valid, stratum 3
ref ID 171.69.2.81, time B6C04E67.6E779000 (18:18:15.431 UTC Thu Feb 27 1997)
our mode client, peer mode server, our poll intvl 128, peer poll intvl 128
root delay 109.51 msec, root disp 377.38, reach 377, sync dist 435.638
delay -3.88 msec, offset 7.7674 msec, dispersion 1.57
precision 2**17, version 3
org time B6C04F19.437D8000 (18:21:13.263 UTC Thu Feb 27 1997)
rcv time B6C04F19.41018C62 (18:21:13.253 UTC Thu Feb 27 1997)
xmt time B6C04F19.41E3EB4B (18:21:13.257 UTC Thu Feb 27 1997)
filtdelay =    -3.88   -3.39   -3.49   -3.39   -3.36   -3.46   -3.37   -3.16
filtoffset =    7.77    6.62    6.60    5.38    4.13    4.43    6.28   12.37
filterror =     0.02    0.99    1.48    2.46    3.43    4.41    5.39    6.36
```

The following example displays the NTP status:

```
Switch# show ntp status
Clock is synchronized, stratum 4, reference is 198.92.30.32
nominal freq is 250.0000 Hz, actual freq is 249.9999 Hz, precision is 2**24
reference time is B6C04F19.41018C62 (18:21:13.253 UTC Thu Feb 27 1997)
clock offset is 7.7674 msec, root delay is 113.39 msec
root dispersion is 386.72 msec, peer dispersion is 1.57 msec
```

Configuring the Clock and Calendar

If no other source of time is available, you can manually configure the current time and date after the system is restarted. The time will remain accurate until the next system restart. Cisco recommends that you use manual configuration only as a last resort.

Note If you have an outside source to which the ATM switch router can synchronize, you do not need to manually set the system clock.

Configuring the Clock

To configure, read, and set the ATM switch router as a time source for a network based on its calendar, perform the following steps in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **clock calendar-valid**	Sets the ATM switch router as the default clock.
Step 2	Switch(config)# **clock summer-time** *zone* **recurring** [*week day month hh:mm week day month hh:mm* [*offset*]]	Configures the system to automatically switch to summer time (daylight savings time), use one of the formats of the **clock summer-time** configuration command.
Step 3	Switch(config)# **clock timezone** *zone hours* [*minutes*]	Configures the system time zone.

To manually read and set the calendar into the ATM switch router system clock, perform the following steps in privileged EXEC mode:

	Command	Purpose
Step 1	Switch# **clock read-calendar**	Reads the calendar.
Step 2	Switch# **clock set** *hh:mm:ss day month year*	Manually sets the system clock.
Step 3	Switch# **clock update-calendar**	Sets the calendar.

To display the system clock information, use the following EXEC command:

Command	Purpose
show clock [*detail*]	Displays the system clock.

Configuring the Calendar

To set the system calendar, use the following privileged EXEC command:

Command	Purpose
calendar set *hh:mm:ss day month year*	Configures the calendar.

To display the system calendar information, use the following EXEC command:

Command	Purpose
show calendar	Displays the calendar setting.

Configuring TACACS

You can configure the ATM switch router to use one of three special TCP/IP protocols related to TACACS: regular TACACS, extended TACACS, or AAA/TACACS+. TACACS services are provided by and maintained in a database on a TACACS server running on a workstation. You must have access to and configure a TACACS server before configuring the TACACS features described in this publication on your Cisco device. Cisco's basic TACACS support is modeled after the original Defense Data Network (DDN) application.

A comparative description of the supported versions follows. Table 4-1 compares the versions by commands.

- TACACS—Provides password checking, authentication, and notification of user actions for security and accounting purposes.
- Extended TACACS—Provides information about protocol translator and ATM switch router use. This information is used in UNIX auditing trails and accounting files.
- AAA/TACACS+—Provides more detailed accounting information as well as more administrative control of authentication and authorization processes.

You can establish TACACS-style password protection on both user and privileged levels of the system EXEC.

Table 4-1 TACACS Command Comparison

Command	TACACS	Extended TACACS	TACACS+
aaa accounting			X
aaa authentication arap			X
aaa authentication enable default			X
aaa authentication login			X
aaa authentication local override			X
aaa authentication ppp			X
aaa authorization			X
aaa new-model			X
arap authentication			X
arap use-tacacs	X	X	
enable last-resort	X	X	
enable use-tacacs	X	X	
login authentication			X
login tacacs	X	X	
ppp authentication	X	X	X
ppp use-tacacs	X	X	X
tacacs-server attempts	X	X	X
tacacs-server authenticate	X	X	
tacacs-server extended		X	
tacacs-server host	X	X	X
tacacs-server key			X
tacacs-server last-resort	X	X	
tacacs-server notify	X	X	
tacacs-server optional-passwords	X	X	
tacacs-server retransmit	X	X	X
tacacs-server timeout	X	X	X

Enabling TACACS and Extended TACACS

This section describes the features available with TACACS and extended TACACS. The extended TACACS software is available using FTP (refer to the README file in the ftp.cisco.com directory).

Note Many original TACACS and extended TACACS commands cannot be used after you have initialized AAA/TACACS+. To identify which commands can be used with the three versions, refer to Table 4-1.

Configuring AAA Access Control with TACACS+

To enable the AAA access control model that includes TACACS+, use the following global configuration command:

Command	Purpose
aaa new-model	Enables the AAA access control model.

Configuring AAA Accounting

To enable the AAA accounting of requested services for billing or security purposes when using TACACS+, perform the following steps in global configuration mode:

	Command	Purpose
Step 1	Switch(config)# **aaa accounting system**	Performs accounting for all system-level events not associated with users, such as reloads.
Step 2	Switch(config)# **aaa accounting network**	Runs accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.
Step 3	Switch(config)# **aaa accounting connection**	Runs accounting for outbound Telnet and rlogin.
Step 4	Switch(config)# **aaa accounting exec**	Runs accounting for Execs (user shells). This keyword might return user profile information such as **autocommand** information.
Step 5	Switch(config)# **aaa accounting commands** *level*	Runs accounting for all commands at the specified privilege level.

Configuring TACACS Server

Refer to the *Security Configuration Guide* for details about the TACACS configuration tasks that include:

- Setting the number of login attempts allowed to the TACACS server
- Enabling extended TACACS mode
- Configuring a TACACS host

Configuring PPP Authentication

Refer to the *Dial Solutions Configuration Guide* for details about the PPP Authentication configuration tasks that include:

- Enabling Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP)
- Enabling an AAA authentication method on an interface

Testing the System Management Functions

This section describes the commands used to monitor and display the system management functions.

Displaying Active Processes

To display information about the active processes, use the following privileged EXEC commands:

Command	Purpose
show processes [**cpu**]	Displays active processes.
show processes memory	Displays memory utilization.

Displaying Protocols

To display the configured protocols, use the following privileged EXEC command:

Command	Purpose
show protocols *type card/subcard/port*	Displays the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, Internet Packet Exchange (IPX), and AppleTalk.

Displaying Stacks

To monitor the stack utilization of processes and interrupt routines, use the following privileged EXEC command:

Command	Purpose
show stacks *number*	Displays system stack trace information.

The **show stacks** display includes the reason for the last system reboot. If the system was reloaded because of a system failure, a saved system stack trace is displayed. This information is of use only to Cisco engineers analyzing crashes in the field. It is included here in case you need to read the displayed statistics to an engineer over the phone.

Displaying Routes

To discover the IP routes that the ATM switch router packets will actually take when traveling to their destination, use the following EXEC command:

Command	Purpose
traceroute [*protocol*] [*destination*]	Displays packets through the network.

Displaying Environment

To display temperature and voltage information on the ATM switch router console, use the following EXEC command:

Command	Purpose
show environment	Displays temperature and voltage information.

Checking Basic Connectivity (Catalyst 8540 MSR)

To diagnose basic ATM network connectivity on the Catalyst 8540 MSR, use the following privileged EXEC command:

Command	Purpose
ping atm interface atm *card/subcard/port vpi* [*vci*] {**end-loopback** [*destination*] | **ip-address** *ip-address* | **seg-loopback** [*destination*]}	Uses **ping** to check the ATM network connection.

Checking Basic Connectivity (Catalyst 8510 MSR and LightStream 1010)

To diagnose basic ATM network connectivity on the Catalyst 8510 MSR and LightStream 1010 ATM switch routers, use the following privileged EXEC command:

Command	Purpose
ping atm interface atm *card/subcard/port vpi* [*vci*] {**atm-prefix** *prefix* | **end-loopback** [*destination*] | **ip-address** *ip-address* | **seg-loopback** [*destination*]}	Uses **ping** to check the ATM network connection.