CHAPTER 6

Configuring System Management Functions

This chapter describes the basic tasks that you need to manage the general system features such as accounting, modeling and management of switch, interface, and connection resources (equivalent bandwidth, buffering) to support the provision of specified traffic classes.

Note For a complete description of the commands mentioned in this chapter, refer to the *LightStream 1010 ATM Switch Command Reference* publication.

The following sections describe the system management functions:

- System Management Tasks
- Configure Privilege Level
- Configure Network Time Protocol
- Configure the Clock and Calendar
- Configure Terminal Access Control Access System
- Test the System Management Functions

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 LightStream 1010 ATM switch.

Configure Alias

To create a command alias, use the **alias** global configuration command. Use the **no alias** command to delete all aliases in a command mode or to delete a specific alias, and to revert to the original command syntax.

Task	Command
Create a command alias.	**alias** *mode alias-name alias-command-line*
Command mode of the original and alias commands.	**alias** *mode*
Command alias.	**alias** *name*
Display all alias commands, or the alias commands in a specified mode.	**show aliases** [*mode*]

Configure buffers

Use the **buffers** global configuration command to make adjustments to initial buffer pool settings and to the limits at which temporary buffers are created and destroyed. Default buffer size of this public buffer pool is 18024 bytes. Use the **no** form of this command to return the buffers to their default size.

Task	Command
Configure buffers.	**buffers** {**small** | **middle** | **big** | **large** | **verylarge** | **huge** | *type number*}
Display statistics for the buffer pools on the network server.	**show buffers [all | alloc [dump]]**

Configure Cisco Discovery Protocol

To specify how often your switch will send Cisco Discover Protocols (CDP) updates, use the **cdp timer** global configuration command. Use the **no** form of this command to revert to the default setting.

Task	Command
Specify the holdtime in seconds, to be sent in packets.	**cdp holdtime** *seconds*
Specify how often your switch will send CDP updates.	**cdp timer** *seconds*
Enable CDP.	**cdp run**

To reset CDP traffic counters to zero (0) on your switch, use the **clear cdp counters** privileged EXEC command. Use the **no** form of this command to revert to the default setting.

Task	Command
Clear CPD counters.	**clear cdp counters**
Clear CPD tables.	**clear cdp table**

To show the CDP configuration use the following **show cdp** privileged EXEC commands:

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

Configure Enable

To log onto the switch at a specified level, use the **enable** EXEC command.

Task	Command
Login enable.	**enable** *level*

To configure the enable password for a given level, use the **enable password** global configuration command. Use the **no** form of this command to remove the enable password for a given level.

Task	Command
Configure the enable password.	**enable password** [**level** *level*] [*encryption-type*] *password*

Configure Load-interval

To change the length of time for which data is used to compute load statistics, use the **load-interval** interface configuration command. Use the **no** form of this command to revert to the default setting.

Task	Command
Configure load interval.	**load-interval** *seconds*

Configure Logging

To log messages to a syslog server host, use the **logging** global configuration command. The **no logging** command deletes the syslog server with the specified address from the list of syslogs.

Task	Command
Configure logging name or IP address of the host to be used as a syslog server.	**logging** *host*
To log 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 buffered**
To limit messages logged to the console based on severity, use the **logging console** global configuration command.	**logging console** *level*

Task	Command
To configure the syslog facility in which error messages are sent, use the **logging facility** global configuration command. To revert to the default of local7, use the **no logging facility** global configuration command.	**logging facility** *facility-type*
To limit 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 monitor** *level*
To control 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 on**
To synchronize unsolicited messages and **debug** output with solicited switch output and prompts for a specific console port line, auxiliary port line, or virtual terminal line, use the **logging synchronous** line configuration command. Use the **no** form of the command to disable synchronization of unsolicited messages and debug output.	**logging synchronous** [level *severity-level* | all] [limit *number-of-buffers*]
To limit 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 trap** *level*

Configure Login Authentication

To enable TACACS+ authentication for logins, use the **login authentication** line configuration command. Use the **no** form of the command to return to the default.

Task	Command
Configure login authentication.	**login authentication** {**default** | *list-name*}

Configure Scheduler

To control the maximum amount of time that can elapse without running the lowest-priority system processes, use the **scheduler** global configuration command. The **no scheduler-interval** command restores the default.

Task	Command
Configure the scheduler allocate integer that specifies the interval, in milliseconds. The minimum interval that you can specify is 500 milliseconds; there is no maximum value.	**scheduler allocate** *milliseconds* *milliseconds*
Configure **scheduler process-watchdog.**	**scheduler process-watchdog** {*hang*|*normal*|*reload*|*terminate*}

Configure Service

Use the **service** command to configure and enable the following global configuration features using the **no service** command to disable the various features.

Task	Command
Configure alignment correction and logging.	**service alignment**
Compress the configuration file.	**service compress-config**
Load config TFTP files.	**service config**
Interpret TTY line numbers in decimal.	**service decimal-tty**
Enable EXEC callback.	**service exec-callback**
Configure delay of the startup of the EXEC on noisy lines.	**service exec-wait**
Allow Finger protocol requests (defined in RFC 742) from the network server.	**service finger**
Hide destination addresses in Telnet command.	**service hide-telnet-addresses**
Enable line number banner for each EXEC.	**service linenumber**
Enable the Nagle congestion control algorithm.	**service nagle**
Allow old scripts to operate with SLIP/PPP.	**service old-slip-prompts**
Enable Packet Assembler Dissembler commands.	**service pad**
Enable encrypt passwords.	**service password-encryption**
Enable mode specific prompt.	**service prompt**
Enable coredump capability of slave IPs.	**service slave-coredump**
Enable log capability of slave IPs.	**service slave-log**
Configure keepalive packets on idle network connections.	**service tcp-keepalives** {**in** | **out**}
Enable small TCP servers (e.g., ECHO).	**service tcp-small-servers**
Set the TCP window to zero (0) when the Telnet connection is idle.	**service telnet-zero-idle**
Displays timestamp debug/log messages.	**service timestamps**
Enable small UDP servers (e.g., ECHO).	**service udp-small-servers**

Configure SNMP

To create or update an access policy, use the **snmp** global configuration command. To remove the specified access policy, use the **no** form of this command.

Task	Command
Configure global access policy.	**snmp-server access-policy** *destination-party source-party context privileges*
Provide a message line identifying the SNMP server serial number.	**snmp-server chassis-id** *text*
Configure the SNMP community access string.	**snmp-server community** *string* [**RO** | **RW**] [*number*]
Configure the system contact (syscontact) string.	**snmp-server contact** *text*
Configure a context record.	**snmp-server context** *context-name context-oid view-name*
Configure recipient of an SNMP trap operation.	**snmp-server host** *host community-string* [**envmon**] [**framerelay**] [**sdlc**] [**snmp**] [**tty**] [**x25**]
Configure system location string.	**snmp-server location** *text*
Configure the largest SNMP packet size permitted when the SNMP server is receiving a request or generating a reply.	**snmp-server packetsize** *byte-count*
Configure a party record.	**snmp-server party** *party-name party-oid* [*protocol-address*] [**packetsize** *size*] [**local | remote**] [**authentication** {**md5** *key* [**clock** *clock*] [**lifetime** *lifetime*] | **snmpv1** *string*}]
Configure message queue length for each trap host.	**snmp-server queue-length** *length*
Configure SNMP message reload.	**snmp-server system-shutdown**
Configure trap message authentication.	**snmp-server trap-authentication** [**snmpv1 | snmpv2**]
Configure how often to resend trap messages on the retransmission queue.	**snmp-server trap-timeout** *seconds*
Configure SNMP v.2 security context using the simplified security conventions method.	**snmp-server userid** *user-id* [**view** *view-name*] [**RO** | **RW**] [**password** *password*]
Configure view entry.	**snmp-server view** *view-name oid-tree* {**included** | **excluded**}
Check status of communications between the SNMP agent and SNMP manager.	**show snmp**

Username Commands

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

Task	Command
Configure username-based authentication system at login.	**username** *name* [**nopassword | password** *encryption-type* **password** *password*]
Configure username-based CHAP authentication system at login.	**username** *name* **password** *secret*

Task	Command
Configure username-based authentication system at login with an additional command to be added.	**username** *name* [**autocommand** *command*]
Configure username-based authentication system at login without escape but with another login prompt.	**username** *name* [**noescape**] [**nohangup**]

Configure Privilege Level

This section describes configuring and displaying the privilege level access to the LightStream 1010. The access privileges can be configured at the global level, for the entire switch, or at the line level, for a specific line.

Configure Privilege Level (Global)

To set the privilege level for a command, use the **privilege level** global configuration command. Use the **no** form of this command to revert to default privileges for a given command.

Task	Command
Set the privilege level.	**privilege** *mode* **level** *level command*

To display your current level of privilege, use the **show privilege** EXEC command.

Task	Command
Display privilege level.	**show privilege**

Configure Privilege Level (Line)

To set the default privilege level for a line, use the **privilege level** line configuration command. Use the **no** form of this command to restore the default user privilege level to the line.

Task	Command
Configure the default privilege level.	**privilege level** *level*

To display your current level of privilege, use the **show privilege** EXEC command.

Task	Command
Display privilege level.	**show privilege**

Configure Network Time Protocol

This section describes configuring the Network Time protocol (NTP) on the LightStream 1010.

To control access to the system NTP services, use the **following** global NTP configuration commands. To remove access control to the system's NTP services, use the **no ntp** command.

To control access to the system NTP services, use the **ntp access-group** global configuration command. To remove access control to the system NTP services, use the **no ntp access-group** command.

Task	Command
Configure NTP access group.	**ntp access-group** {**query-only** | **serve-only** | **serve** | **peer**} *access-list-number*

To enable NTP authentication, use the **ntp authenticate** global configuration command. Use the **no** form of this command to disable the feature.

Task	Command
Enable NTP authentication.	**ntp authenticate**
Define an authentication key.	**ntp authentication-key** *number* **md5** *value*

To specify that a specific interface should send NTP broadcast packets, use the **ntp broadcast** interface configuration command. Use the **no** form of the command to disable this capability.

Task	Command
Specify that a specific interface should send NTP broadcast packets.	**ntp broadcast** [**version** *number*]
Allows the system to receive NTP broadcast packets.	**ntp broadcast client**
Allows the system to receive NTP broadcast packets.	**ntp broadcastdelay** *microseconds*

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. The system uses the **no** form of this command to revert to the default.

Task	Command
Do not enter this command.	**ntp clock-period** *value*

Caution Do not enter this 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, use the **ntp disable** interface configuration command. To enable receipt of NTP packets on an interface, use the **no ntp disable** command.

Task	Command
Disable the NTP receive interface.	**ntp disable**

To configure the switch as a NTP master clock to which peers synchronize themselves when an external NTP source is not available, use the **ntp maste**r global configuration command. To disable the master clock function, use the **no ntp master** command.

Task	Command
Configure the switch as an NTP master clock.	**ntp master** [*stratum*]

To configure the switch as a NTP peer that receives its clock synchronization from an external NTP source, use the **ntp peer** global configuration command. To disable the peer clock function, use the **no ntp peer** command.

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

To allow the switchs system clock to be synchronized by a time server, use the **ntp server** global configuration command. To disable this capability, use the **no ntp server** command.

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

To use a particular source address in NTP packets, use the **ntp source** global configuration command. Use the **no** form of this command to remove the specified source address.

Task	Command
Configure a particular source address in NTP packets.	**ntp source** *interface*

If you want to authenticate the identity of a system to which NTP will synchronize, use the **ntp trusted-key** global configuration command. Use the **no** form of this command to disable authentication of the identity of the system.

Task	Command
Configure NTP synchronize number.	**ntp trusted-key** *key-number*

To periodically update the switch calendar from NTP, use the **ntp update-calendar** global configuration command. Use the **no** form of this command to disable this feature.

Task	Command
Update NTP calendar.	**ntp update-calendar**

To show the status of NTP associations, use the **show ntp associations** EXEC command.

Task	Command
Display NTP associations.	**show ntp associations** [**detail**]
Display NTP status.	**show ntp status**

Configure 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. We recommend that you use manual configuration only as a last resort.

To set up time services, complete the following tasks as needed. If you have an outside source to which the LightStream 1010 can synchronize, you do not need to manually set the system clock.

- Configure the Clock
- Configure Calendar

Configure the Clock

To configure, read, and set the LightStream 1010 ATM switch as a time source for a network based on its calendar, use the **clock** global configuration command. Use the **no** form of this command to set the switch so that the calendar is not an authoritative time source. Use the **no** form of this command to configure the switch not to automatically switch to summer time.

Task	Command
Set the LightStream 1010 as the default clock.	**clock calendar-valid**
Configure the system to automatically switch to summer time (daylight savings time), use one of the formats of the **clock summer-time** configuration command. Use the **no** form of this command to configure the switch to not automatically switch to summer time.	**clock summer-time** *zone* recurring [*week day month hh:mm week day month hh:mm* [*offset*]]

To manually read and set the calendar into the LightStream 1010 system clock, use the **clock read-calendar** EXEC command.

Task	Command
Manually read the calendar into the switch.	**clock read-calendar**
Manually set the system clock.	**clock set** *hh:mm:ss day month year*
Manually set the system clock.	**clock set** *hh:mm:ss month day year*
Set the calendar.	**clock update-calendar**

To display the system clock, use the **show clock** EXEC command.

Task	Command
Display the system clock.	**show clock** *[detail]*

Configure Calendar

To set the system calendar, use the **calendar set** EXEC command.

Task	Command
Configure the calendar.	**calendar set** *hh:mm:ss day month year*
Display the calendar setting.	**show calendar**

Configure Terminal Access Control Access System

You can configure the LightStream 1010 to use one of three special TCP/IP protocols related to Terminal Access Controller Access Control System (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. Our basic TACACS support is modeled after the original Defense Data Network (DDN) application.

A comparative description of the supported versions follows. Table 6-1 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 LightStream 1010 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 6-1 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**

Command	TACACS	Extended TACACS	TACACS+
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

Enable TACACS and Extended TACACS

The following sections describe the features available with TACACS and Extended TACACS. The Extended TACACS software is available using FTP (see the README file in the *ftp.cisco.com* directory).

Note Many original TACACS and extended TACACS commands cannot be used once you have initialized AAA/TACACS+. To identify which commands can be used with the three versions, refer to Table 6-1.

The following sections describe TACACS configuration:

- Configure AAA Accounting
- Configure aaa new-model
- Configure Tacacs-server
- Configure PPP Authentication

Configure AAA Accounting

To enable the AAA accounting of requested services for billing or security purposes when using TACACS+, use the **aaa accounting** global configuration command. Use the **no** form of this command to disable accounting.

Task	Command
Perform accounting for all system-level events not associated with users, such as reloads.	**aaa accounting system**
Run accounting for all network-related service requests, including SLIP, PPP, PPP NCPs, and ARAP.	**aaa accounting network**
Run accounting for outbound Telnet and rlogin.	**aaa accounting connection**
Run accounting for Execs (user shells). This keyword might return user profile information such as autocommand information.	**aaa accounting exec**
Run accounting for all commands at the specified privilege level.	**aaa accounting command**

Task	Command
Send a start record accounting notice at the beginning of a process and a stop record at the end of a process. The start accounting record is sent in the background. The requested user process begins regardless of whether or not the start accounting record was received by the accounting server.	{**start-stop tacacs+**
As in **start-stop**, sends both a start and a stop accounting record to the accounting server. However, if you use the **wait-start** keyword, the requested user service does not begin until the start accounting record is acknowledged. A stop accounting record is also sent.	**wait-start tacacs+**
Sends a stop record accounting notice at the end of the requested user process.	**stop-only tacacs+**

Configure aaa new-model

To enable the AAA access control model that includes TACACS+, issue the **aaa new-model** global configuration command. Use the **no** form of the command to disable this functionality.

Task	Command
Enable the AAA access control model.	**aaa new-model**

Configure Tacacs-server

To configure a Terminal Access Control Access System (TACACS) use the **tacacs** global commands. Use the **no tacacs** command with the appropriate arguments to remove an entry.

Task	Command
Configure the number of login attempts allowed.	**tacacs-server attempts** *count*
Configure if user may perform an action.	**tacacs-server authenticate** {**connection** [**always**] | **enable** | **slip** [**always**] [**access-lists**]}
Configure extended TACACS mode.	**tacacs-server extended**
Configure a TACACS host.	**tacacs-server host** *name*
Configure network server to request privileged password as verification.	**tacacs-server last-resort** {**password** | **succeed**}
Configure transmission to the TACACS server.	**tacacs-server notify** {**connection** [**always**] | **enable** | **logout** [**always**] | **slip** [**always**]}
Configure first TACACS request to a TACACS server be made *without* password verification.	**tacacs-server optional-passwords**
Configure the initial TACACS request to a TACACS server be made *without* password verification.	**tacacs-server optional-passwords**
Configure number of times the system software will search the list of TACACS server hosts.	**tacacs-server retransmit** *retries*
Configure interval that the server waits for a server host to reply.	**tacacs-server timeout** *seconds*

Configure PPP Authentication

Use the **ppp authentication** interface configuration command to enable Challenge Handshake Authentication Protocol (CHAP) or Password Authentication Protocol (PAP) and to enable an AAA authentication method on an interface. Use the **no** form of the command to disable this authentication.

Task	Command
Configure ppp authentication.	**ppp authentication** {**chap** | **pap**} [**if-needed**] [*list-name*]
Enable the PPP authentication for TACACS.	**ppp use-tacacs** [**single-line**]

To enable TACACS to determine whether a user can access the privileged command level, use the **enable use-tacacs** global configuration command. Use the **no** form of this command to disable TACACS verification.

Task	Command
Enable TACACS.	**enable use-tacacs**

Test the System Management Functions

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

Show Active Processes

Use the **show processes** EXEC command to display information about the active processes.

Task	Command
Display active processes.	**show processes** [**cpu**]
Display memory utilization.	**show processes memory**

Show Protocols

Use the **show protocols** EXEC command to display the configured protocols.

This command shows the global and interface-specific status of any configured Level 3 protocol; for example, IP, DECnet, Internet Packet Exchange (IPX), and AppleTalk.

Task	Command
Display protocols.	**show protocols**

Show Stacks

Use the **show stacks** EXEC command to monitor the stack utilization of processes and interrupt routines. Its 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.

Task	Command
Displays system stack trace information.	**show stacks**

Use Trace

Use the **trace** EXEC command to discover the IP routes the switch packets will actually take when traveling to their destination.

Task	Command
Display switch packets through the network.	**trace** [*protocol*] [*destination*]

Show Environment

Use the **show environment** EXEC command to display temperature and voltage information on the switch console.

Task	Command
Display temperature and voltage information.	**show environment**
Display all temperature and voltage information.	**show environment all**
Display last logs of the last measured value from each of the six test points to internal nonvolatile memory.	**show environment last**
Display environmental measurements and a table that lists the ranges of environment measurement.	**show environment table**

Use Packet Internet Groper

Use the packet internet groper (**ping**) privileged EXEC command to diagnose basic ATM and IP network connectivity.

Task	Command
Use PING to check the ATM network connection.	**ping atm interface atm** *card/sub_card/port*[*.vpt*] *vpi vci*
Use PING to check the IP network connection.	**ping [ip]** [*protocol*] {*host* | *address*}