CHAPTER 4

Initially Configuring the LightStream 1010 ATM Switch

This chapter discusses the initial configuration of the LightStream 1010 ATM switch. Because the LightStream 1010 offers true plug-and-play operation, most users may not need to perform any of these procedures.

The LightStream 1010 is shipped with the ATM address autoconfigured to an address assigned by Cisco Systems. This allows the switch to automatically configure attached end-systems using the ILMI protocol and to automatically establish itself as a node in a single-level PNNI routing domain.

Note The default software image for the LightStream 1010 will contain only the IISP routing protocol. This is suitable for small networks that do not require the sophistication of the PNNI protocols. A separate orderable image will contain both PNNI and IISP protocols. The PNNI protocol provides the route dissemination mechanism for complete plug-and-play capability.

The ILMI and PNNI protocols, when used with such IP address autoconfiguration mechanisms as BOOTP, allow the LightStream 1010 to be entirely self-configured. Through network management applications and the text-based command line interface (CLI), the switch's network operator will have the capability, if desired, to configure and customize all aspects of the operation of the switch.

An IP address must be assigned to allow up to eight simultaneous Telnet sessions to connect to the switch or to use SNMP network management for the switch. The Ethernet IP address can be assigned either manually or by a BOOTP server. See the section "Configure IP Interface Parameters."

Note If your Telnet station or SNMP network management workstation is on a different network from the switch, a static routing table entry must also be added to the routing table. Use the **ip route** command to set the static routing table entry.

For definitions of all commands discussed in this chapter, refer to the publication *LightStream 1010 ATM Switch Command Reference.*

The following sections describe the LightStream 1010 initial configuration:

- Before You Begin Configuration
- BOOTP Server Configuration
- ATM Address Configuration
- Configure the Interfaces

- Configure the Network Routing
- Configure the System Information
- Configure SNMP Management
- Store the Configuration
- Test the Configuration

Before You Begin Configuration

If you want to configure some additional features, you might need the following information before you can begin your LightStream 1010 configuration:

- If you want to configure a BOOTP server to inform the switch of its Ethernet IP address and mask, you need the media access control (MAC) address of the Ethernet port.
- If you want to configure a new ATM address for the switch (an autoconfigured ATM address is assigned by Cisco Systems), you will need an ATM address assigned by your system administrator.
- If you are not using BOOTP, you will need an IP address.
- If you want to configure the Ethernet port on the ASP, you will need a Netmask address.
- If you want to configure the Ethernet port on the ASP, you will need Broadcast address.

To help configure your switch you should have already completed the worksheets in the section "Port Configuration Worksheets" in the appendix "Configuration Worksheets" in the *LightStream 1010 ATM Switch User Guide* publication.

Note You should have completed all interface and power connections described in the chapter "Installing the LightStream 1010 ATM Switch" in the *LightStream 1010 ATM Switch User Guide* publication before beginning to configure the switch.

Verify Installed LightStream 1010 Software and Hardware

When you first power up your console and LightStream 1010, a screen similar to the following appears:

```
               Restricted Rights Legend

   Use, duplication, or disclosure by the Government is
   subject to restrictions as set forth in subparagraph
   (c) of the Commercial Computer Software - Restricted
   Rights clause at FAR sec. 52.227-19 and subparagraph
   (c) (1) (ii) of the Rights in Technical Data and Computer
   Software clause at DFARS sec. 252.227-7013.

              cisco Systems, Inc.
              170 West Tasman Drive
              San Jose, California 95134-1706



   Cisco Internetwork Operating System Software
   IOS (tm) IISP Software (LS1010-WI-M), Version 11.1(1.083)
   Copyright (c) 1986-1996 by cisco Systems, Inc.
   Compiled Wed 10-Apr-96 06:11 by
   Image text-base: 0x600108C0, data-base: 0x602E8000
```

Note In the previous example,
LS Software (LS1010--WI-M) means the IISP software image is loaded.
LS Software (LS1010-WP-M) means the PNNI software image is loaded.

The first section of the script displays the banner information, including the software version.

The next portion of the script lists installed hardware configuration.

```
   cisco ASP1 (R4600) processor with 16384K bytes of memory.
   R4600 processor, Implementation 32, Revision 2.0
   Last reset from power-on
   1 Ethernet/IEEE 802.3 interface.
   16 ATM network interfaces.
   125K bytes of non-volatile configuration memory.

   8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
   8192K bytes of Flash internal SIMM (Sector size 256K).


   Switch>
```

The LightStream 1010 should be operating correctly and transferring data.

Note If an rommon > prompt appears your switch requires a manual boot to recover. See the section "Manually Boot from Flash memory" in the chapter "Loading System Images, Software Images, and Configuration Files."

BOOTP Server Configuration

The LightStream 1010 Ethernet IP address can automatically be assigned using the BOOTP protocol by adding the MAC and IP addresses of the Ethernet port to the BOOTP server configuration file. When the switch boots, it automatically retrieves the IP address from the BOOTP server.

The switch performs a BOOTP request *only* if the current IP address is set to 0.0.0.0. (This is the default for a new switch or a switch that has had its configuration file cleared using the **erase startup-config** command.)

To allow your LightStream 1010 to retrieve its IP address from a BOOTP server, you must first determine the MAC address of the switch and add that MAC address to the BOOTP configuration file on the BOOTP server. The following tasks provide an example of creating a BOOTP server configuration file:

Task	Command
Install the BOOTP server code on the workstation, if it is not already installed.	**None**
Determine MAC address from label on chassis.	None
Add an entry in the BOOTP configuration file (usually */usr/etc/bootptab*) for each switch. Press Return after each entry to create a blank line between each entry. Figure 4-1 is an example of a server BOOTP configuration file.	None
Restart the LightStream 1010 to automatically request the IP address from the BOOTP server.	**restart**

Figure 4-1 is an example of a BOOTP configuration file with the LightStream 1010 ATM switch entry added at the end of the example.

Figure 4-1 Example of a Server BOOTP Configuration File

```
# /etc/bootptab: database for bootp server (/etc/bootpd)
#
# Blank lines and lines beginning with '#' are ignored.
#
# Legend:
#
#       first field -- hostname
#                       (may be full domain name and probably should be)
#
#       hd -- home directory
#       bf -- bootfile
#       cs -- cookie servers
#       ds -- domain name servers
#       gw -- gateways
#       ha -- hardware address
#       ht -- hardware type
#       im -- impress servers
#       ip -- host IP address
#       lg -- log servers
#       lp -- LPR servers
#       ns -- IEN-116 name servers
#       rl -- resource location protocol servers
#       sm -- subnet mask
#       tc -- template host (points to similar host entry)
#       to -- time offset (seconds)
#       ts -- time servers
```

```
#
# Be careful about including backslashes where they're needed.  Weird (bad)
# things can happen when a backslash is omitted where one is intended.
#


# First, we define a global entry which specifies the stuff every host uses.


<information deleted>

###############################################################################
# Start of individual host entries
###############################################################################
Switch:         tc=netcisco0:   ha=0000.0ca7.ce00:      ip=192.31.7.97:
dross:          tc=netcisco0:   ha=00000c000139:        ip=192.31.7.26:

<information deleted>
```

ATM Address Configuration

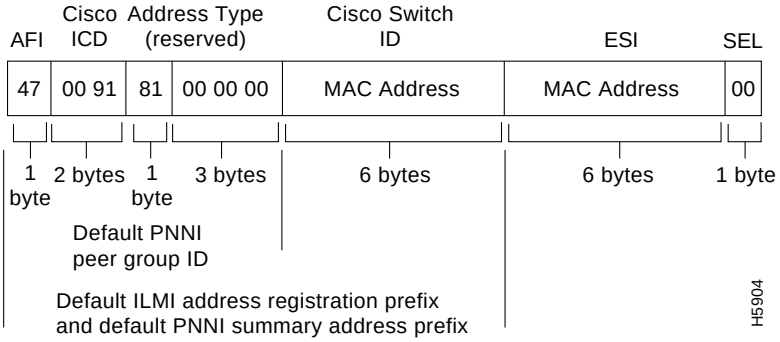
The LightStream 1010 ATM switch is autoconfigured with an ATM address using a hierarchical addressing model similar to the OSI network service access point (NSAP) addresses.

Note The most important rule in the addressing scheme is to maintain the uniqueness of the address across very large networks.

Autoconfigured ATM Addressing Scheme

During the initial startup the LightStream 1010 generates an ATM address using the defaults shown in Figure 4-2:

Figure 4-2 ATM Address Format



- Authority Format Identifier (AFI)—1 byte
- Cisco specific International Code Designator (ICD)—2 bytes
- Cisco specific information—4 bytes
- Cisco switch ID—6 bytes (used to distinguish multiple switches)

Note This first 13 bytes of the address is a switch prefix used by ILMI in assigning addresses to end stations connected to UNI ports.

- MAC address of the switch—6 bytes (used to distinguish multiple End System Identifier (ESI) addresses)

Note Both MAC address fields are the same but they may not be the same as the address on the chassis label.

- Selector equals 0—1 byte

Default Address Format Features and Implications

Using the default address format has the following features and implications:

- The default address format may also be used to manually configure other switches to allow them to be used in a single-level PNNI routing domain consisting primarily of autoconfigured Cisco ATM switches. A globally unique MAC address must be used to generate the ATM address.
- The same MAC address can be used for bytes 8 through 13 and bytes 14 through 19.
- This address assignment format is relatively flat. To achieve scalable ATM routing, addresses will need to be changed when connecting to a large ATM network with multiple levels of PNNI hierarchy.
- Summary addresses less than 13 bytes long should *not* be used with autoconfigured ATM addresses. Other switches with autoconfigured ATM addresses matching the summary may exist outside of the default peer group.

Manually Setting the ATM Address

To configure a new ATM address that replaces the previous ATM address, when running IISP software only, see the section “Configure the ATM Address” in the chapter “Configuring ILMI.”

To configure a new ATM address that replaces the previous ATM address and generates a new PNNI node ID and peer group ID, see the section “Configure PNNI Node” in the chapter “Configuring PNNI.”

Multiple addresses can be configured for a single switch and this configuration can be used during ATM address migration. ILMI registers end systems with multiple prefixes during this period until an old address is removed. PNNI automatically summarizes all of the switch prefixes in its reachable address advertisement.

If operation with ATM addresses other than the autoconfigured ATM address is desired, use the **atm address** command to manually assign a 20-byte ATM address to the switch. The **atm address** command *address_template* variable can be a full 20-byte address or a 13-byte prefix followed by ellipsis (...). Entering the ellipsis will automatically add one of the switch’s 6-byte MAC addresses in the ESI portion and 0 in the selector portion of the address.

Caution ATM addressing may lead to conflicts if not configured correctly. The correct address must always be present. For instance, if you are configuring a new ATM address, the old one must be completely removed from the configuration.

Configure the Interfaces

When the switch is powered on initially without any previous configuration data, the ATM interfaces are automatically configured on the physical ports. ILMI and the physical card type are used to automatically derive the ATM interface type, UNI version, maximum VPI and VCI bits, ATM interface side, and ATM UNI type.

Default ATM Interface Configuration Without Autoconfiguration

If ILMI has been disabled or if the connecting end node does not support ILMI, the following defaults are assigned to all interfaces:

- ATM interface type = *UNI*
- UNI version = 3.0
- Maximum VPI bits = 8
- Maximum VCI bits = 14
- ATM interface side = *network*
- ATM UNI type = *private*

The following PAM types have specific defaults assigned:

OC3 PAM:

- Framing = sts-3c
- Clock-source = free-running
- Synchronous Transfer Signal (STS) -stream scrambling = on
- Cell payload scrambling = on

OC12 PAM:

- Framing = sts-12c
- Clock-source = free-running
- STS-stream scrambling = on
- Cell payload scrambling = on

DS3 PAM:

- Framing = cbit-adm
- Cell payload scrambling = off
- Clock-source = free-running
- Line build out (LBO) = short
- Auto-ferf on loss of signal (LOS) = on
- Auto-ferf on out of frame (OOF) = on
- Auto-ferf on red = on

- Auto-ferf on loss of cell delineation (LCD) = on
- Auto-ferf on alarm indication signaling (AIS) = on
- **E3 PAM**:
- Framing = g.751 plcp
- Cell payload scrambling = off
- Clock-source = free-running
- Auto-ferf on LOS = on
- Auto-ferf on out of frame (OOF) = on
- Auto-ferf on red = on
- Auto-ferf on LCD = on
- Auto-ferf on AIS = on

You can accept the default ATM interface configuration or overwrite the default interface configuration using the command line interface commands. These commands are described in the section "Configuring Virtual Connections."

Modify Default for Physical Layer Configuration of an ATM Interface

This section describes modifying an ATM interface from the default configuration listed in the section "Default ATM Interface Configuration Without Autoconfiguration."

The following example describes modifying an OC3 interface from the default settings to the following:

- Disable scrambling cell-payload.
- Disable scrambling sts-streaming.
- Change SONET mode of operation from synchronous time stamp (STS) 3c mode to synchronous transport mode (STM)-1.

To change the configuration of the example interface, use the following EXEC commands using the **no** form of this command to disable:

Task	Command
At the privileged EXEC prompt, enter configuration mode from the terminal.	**configure**[1] [**terminal**]
Select the physical interface to be configured.	**interface atm** *card/sub_card/port*
Disable cell-payload scrambling.	**no scrambling cell-payload**
Disable STS-stream scrambling.	**no scrambling sts-stream**
Configure SONET mode as SDH/STM-1.	**sonet** {**stm-1**|**sts-3c**}
Exit configuration mode.	**exit**

1. This command is documented in the *LightStream 1010 ATM Switch Command Reference* publication.

Example

The following example disables cell-payload scrambling and STS-stream scrambling and changes the SONET mode of operation to SDH/STM-1 of OC3 physical interface 0/0/0:

```
Switch(config)#interface atm 0/0/0
Switch(config-if)#no scrambling cell-payload
Switch(config-if)#no scrambling sts-stream
Switch(config-if)#sonet stm-1
Switch(config-if)#exit
Switch#
```

To change any of the other physical interface default configurations refer to the commands in the *LightStream 1010 ATM Switch Command Reference* for detailed command syntax information.

Use show controller and show running-config Commands to Display the Interface Physical Layer Configuration

To display the physical interface configuration, use the following commands:

Task	Command
Show the physical layer configuration.	**show controllers atm** *card/sub_card/port*
Show physical layer scrambling configuration.	**show running-config**

Examples

The following example displays the OC3 physical interface configuration after modification of the defaults using the **show controllers** command:

```
Switch#show controller atm 0/0/0
IF Name: ATM0/0/0    Chip Base Address: A8808000
Port type: 155UTP    Port rate: 155 Mbps    Port medium: UTP
Port status:PATH LOP    Loopback:PIF    Flags:8000
TX Led: Traffic Pattern    RX Led: Traffic Pattern
TX clock source:  free-running
Framing mode:  stm-1

OC3 counters:

  Key: txcell - # cells transmitted
       rxcell - # cells received
       b1     - # section BIP-8 errors
       b2     - # line BIP-8 errors
       b3     - # path BIP-8 errors
       ocd    - # out-of-cell delineation errors - not implemented
       g1     - # path FEBE errors
       z2     - # line FEBE errors
       chcs   - # correctable HEC errors
       uhcs   - # uncorrectable HEC errors

txcell:8501, rxcell:1165
b1:0, b2:0, b3:0, ocd:0
g1:0, z2:0, chcs:0, uhcs:0

OC3 errored secs:
b1:0, b2:0, b3:0, ocd:0
g1:0, z2:0, chcs:0, uhcs:0

OC3 error-free secs:
b1:0, b2:0, b3:0, ocd:0
g1:0, z2:0, chcs:0, uhcs:0

Clock reg:80
```

```
  mr 0x30, mcfgr 0x70, misr 0xE0, mcmr 0xEF,
  mctlr 0x48, cscsr 0x50, crcsr 0x20, rsop_cier 0x40,
  rsop_sisr 0x40, rsop_bip80r 0x00, rsop_bip81r 0x00, tsop_ctlr 0xC0,
  tsop_diagr 0xC0, rlop_csr 0x00, rlop_ieisr 0x0C, rlop_bip8_240r 0x00,
  rlop_bip8_241r 0x00, rlop_bip8_242r 0x00, rlop_febe0r 0x00, rlop_febe1r 0x00,
  rlop_febe2r 0x00, tlop_ctlr 0x80, tlop_diagr 0x80, rpop_scr 0x64,
  rpop_isr 0x67, rpop_ier 0x43, rpop_pslr 0x00, rpop_pbip80r 0x00,
  rpop_pbip81r 0x00, rpop_pfebe0r 0x00, rpop_pfebe1r 0x00, tpop_cdr 0x00,
  tpop_pcr 0x00, tpop_ap0r 0x00, tpop_ap1r 0x08, tpop_pslr 0x13,
  tpop_psr 0x00, racp_csr 0x86, racp_iesr 0x10, racp_mhpr 0x00,
  racp_mhmr 0x00, racp_checr 0x00, racp_uhecr 0x06, racp_rcc0r 0x00,
  racp_rcc1r 0x00, racp_rcc2r 0x00, racp_cfgr 0xFC, tacp_csr 0x06,
  tacp_iuchpr 0x01, tacp_iucpopr 0x6A, tacp_fctlr 0x00, tacp_tcc0r 0x00,
  tacp_tcc1r 0x00, tacp_tcc2r 0x00, tacp_cfgr 0x08,

Switch#
```

The following example displays the OC3 physical layer scrambling configuration after modification of the defaults using the **show running-config** command:

```
Switch#show running-config
Building configuration...

Current configuration:
!
version 11.1
no service pad
service exec-wait
service udp-small-servers
service tcp-small-servers
!
hostname Switch
!
clock summer-time pdt recurring 4 Sun Apr 2:00 last Sun Oct 2:00
boot buffersize 50000
boot system flash ls1010-wp-mz.111-1.226
boot bootldr slot0:ls1010-wp-mz.111-1.226
!
ip host-routing
ip rcmd rcp-enable
ip rcmd rsh-enable
ip rcmd remote-host dplatz 171.69.1.129 dplatz enable
ip rcmd remote-host root 171.69.1.129 root enable
ip rcmd remote-username dplatz
ip rcmd source-interface Ethernet2/0/0
atm over-subscription-factor 16
atm service-category-limit cbr 3000
atm qos uni3-default  cbr max-cell-loss-ratio 12
atm address 47.0091.8100.0000.0041.0b0a.1081.0041.0b0a.1081.00
atm address 47.0091.8100.0000.0060.3e5a.db01.0060.3e5a.db01.00
atm address 47.0091.8100.5670.0000.0000.1122.0040.0b0a.1081.00
atm router pnni
 max-admin-weight-percentage 300
 background-routes
 administrative-weight linespeed
 statistics call
 node 1 level 56 lowest
  redistribute atm-static
!
!
interface ATM0/0/0
 loopback pif
 no keepalive
 no atm address-registration
```

```
 no atm ilmi-enable
 atm nni
 atm pvp 99
 atm prefix 47.0091.8100.0000.0003.c386.b301...
 atm pnni node 1
 sonet stm-1
 no scrambling sts-stream
 no scrambling cell-payload
!
--More--
```

Configure IP Interface Parameters

IP addresses may be configured on the LightStream 1010 ASP interfaces. Each IP address is configured using one of the following purposes:

- Ethernet port—can be configured either from the BOOTP server or using the **interface ethernet 2/0/0 ip address** command.
- Classical IP over ATM—See the section "Configure IP Over ATM Example" in the chapter "Configuring the LANE and IP Over ATM Clients."
- LANE client—See the section "Configure LAN Emulation Client Example" in the chapter "Configuring the LANE and IP Over ATM Clients."
- SLIP/PPP—See the chapter "Configuring Terminal Lines and Modem Support."

Note These IP connections are only used for network management.

Configure the interface to communicate with the switch CPU (interface 2/0/0) or Ethernet interface 2/0/0 using the following information as a guide:

Provide the IP address and subnet mask bits for the interface as follows:

- IP address

Internet addresses are 32-bit values assigned to hosts that use the IP protocols. These addresses are in dotted decimal format (four decimal numbers separated by periods) such as 192.17.5.100. Each number is an 8-bit value between 0 and 255. The following is a summary of IP addressing concepts for those who are somewhat familiar with IP addressing.

The addresses are divided into three classes; the classes differ in the number of bits allocated to the *network* and *host* portions of the address.

The Class A Internet address format allocates the highest 8 bits to the network field and sets the highest-order bit to 0 (zero). The remaining 24 bits form the host field.

The Class B Internet address allocates the highest 16 bits to the network field and sets the two highest-order bits to 1, 0. The remaining 16 bits form the host field.

The Class C Internet address allocates the highest 24 bits to the network field and sets the three highest-order bits to 1, 1, 0. The remaining 8 bits form the host field.

Default: None.

Action: Enter your Internet address in dotted decimal format for each interface you plan to configure.

- Subnet mask bits

Subnetting is an extension of the Internet addressing scheme, which allows multiple physical networks to exist within a single Class A, B, or C network. The usual practice is to use a few of the far left bits in the host portion of the network address for a subnet field. The subnet mask determines whether subnetting is in effect on a network.

Internet addressing conventions allow a total of 24 host bits for Class A addresses, a total of 16 host bits for Class B addresses, and a total of 8 host bits for Class C addresses. When you are further subdividing your network (that is, subnetting your network), the number of host addressing bits is divided between subnetting bits and actual host address bits. You must specify a minimum of two host address bits, or the subnetwork could not be populated by hosts. Therefore, the **setup** command facility permits you to specify up to 22 host bits for Class A subnetting, 14 bits for Class B subnetting, and 6 bits for Class C subnetting. Table 4-1 provides a summary of these subnetting parameters.

Table 4-1 Summary of Subnetting Parameters

			Host Bits	
First Class	**First Byte**	**Network Bits**	**Max Subnet Bits**	**Min Address Bits**
A	1–126	8	22	2
B	128–191	16	14	2
C	192–223	24	6	2

Default: 0.

Note Because all zeros in the host field specifies the entire network, subnetting with subnet address 0 is illegal and is strongly discouraged.

Define subnet mask bits as a decimal number between 0 and 22 for Class A addresses, 0 and 14 for Class B addresses, or 0 and 6 for Class C addresses. Do not specify 1 as the number of bits for the subnet field. That specification is reserved by Internet conventions.

Hot-Swapping Default Configuration

Hot-swapping or removing an individual Port Adapter Module (PAM) after it has been configured from the LightStream 1010 affects the configuration of the switch differently if the PAM is replaced with the same type and speed module or if the PAM is replaced with a different type and speed module. Both situations will be discussed in the following sections.

Replace a PAM with the Same PAM Type

This section describes hot-swapping a PAM and replacing it with the same speed and type of PAM. It also describes the configured state of the connections during and after hot-swapping.

In this example a 155 multimode PAM is configured in card slot 4, sub-card 0, with cross-connect PVCs to a 622 multimode interface in slot 4, sub-card 1and to the ASP interface 2/0/0, as shown in Figure 4-3.

Figure 4-3 Hot-Swapping PAM Example with PAM Installed

```
switch#show hardware

LS1010 named Switch, Date: 10:51:01 UTC Wed May 1 1996

Slot Ctrlr-Type    Part No.  Rev  Ser No  Mfg Date  RMA No. Hw Vrs  Tst EEP
---- ------------  ---------- -- -------- -------- -------- ------- --- ---
4/0  155MM PAM     73-1496-03 00 03115013  2/27/96 00-00-00   3.0     0   2
4/1  622MM PAM     73-1864-01 00 00000003  4/08/96 00-00-00   1.1     0   2
2/0  ATM Swi/Proc  73-1402-02 06 00000001  8/01/95 00-00-00   2.2     0   2
Switch#show atm vc interface atm 4/1/0
Interface    VPI     VCI     Type   X-Interface  X-VPI   X-VCI   Status
ATM4/1/0     0       5        PVC     ATM2/0/0     0       44      UP
ATM4/1/0     0       16       PVC     ATM2/0/0     0       45      UP
ATM4/1/0     0       18       PVC     ATM2/0/0     0       46      UP
ATM4/1/0     0       33       PVC     ATM4/0/0     0       34      UP
ATM4/1/0     0       34       PVC     ATM4/0/1     0       34      UP
```

If the 155 multimode PAM is removed from card slot 4, sub-card 0, the interface ports are changed to administratively down as show in Figure 4-4.

Figure 4-4 Hot-Swapping PAM Example with PAM Removed

```
Switch#
%OIR-6-REMCARD: Card removed from slot 4, subcard 0, interfaces disabled
%LINK-5-CHANGED: Interface ATM4/0/0, changed state to administratively down
%LINK-5-CHANGED: Interface ATM4/0/1, changed state to administratively down
%LINK-5-CHANGED: Interface ATM4/0/2, changed state to administratively down
%LINK-5-CHANGED: Interface ATM4/0/3, changed state to administratively down
Switch#
```

If the 155 multimode PAM is reinstalled in card slot 4, sub-card 0, the interface connections are changed to up as show in Figure 4-5.

Figure 4-5 Hot-Swapping PAM Example with PAM Reinstalled

```
Switch#
%OIR-6-INSCARD: Card inserted in slot 4, subcard 0,  interfaces administratively shutdown
%LINEPROTO-5-UPDOWN: Line protocol on Interface ATM4/0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface ATM4/0/1, changed state to up
%LINK-3-UPDOWN: Interface ATM4/0/0, changed state to up
%LINK-3-UPDOWN: Interface ATM4/0/1, changed state to up
```

Note If a different speed and type PAM is inadvertently installed in the PAM slot but not configured, then the same speed and type PAM as previously configured is reinserted the original connections will be reestablished.

Replace a PAM with a Different PAM Type

This section describes hot-swapping a PAM and replacing it with a different speed and type of PAM. It also describes the configured state of the connections during and after hot-swapping.

In this example a 155 multimode PAM is configured in card slot 4, sub-card 0, with cross-connect PVCs to a 622 multimode interface in slot 4, sub-card 1 and to the ASP interface 2/0/0, as in Figure 4-3.

If the 155 multimode PAM is removed from card slot 4, sub-card 0, the cross-connections are changed to administratively down as show in Figure 4-4.

If an E3 PAM is inserted into card slot 4, sub-card 0, the cross-connections between 4/0 and 4/1 are changed to removed as show in Figure 4-6.

Figure 4-6 Hot-Swapping PAM Example with Different Type PAM Reinstalled

```
Switch#show hardware

LS1010 named Switch, Date: 10:55:10 UTC Wed May 1 1996

Slot Ctrlr-Type    Part No.  Rev  Ser No  Mfg Date  RMA No. Hw Vrs  Tst EEP
---- ------------  ---------- -- -------- -------- -------- ------- --- ---
4/0  E3 PAM        73-1573-01 12 02828094  8/01/95 00-00-00   1.0     0   2
4/1  622MM PAM     73-1864-01 00 00000003  4/08/96 00-00-00   1.1     0   2
2/0  ATM Swi/Proc  73-1402-02 06 00000001  8/01/95 00-00-00   2.2     0   2
Switch#show atm vc interface atm 4/1/0
Interface    VPI     VCI     Type   X-Interface  X-VPI   X-VCI   Status
ATM4/1/0     0       5        PVC     ATM2/0/0     0       44      UP
ATM4/1/0     0       16       PVC     ATM2/0/0     0       45      UP
ATM4/1/0     0       18       PVC     ATM2/0/0     0       46      UP
ATM4/1/0     0       33       PVC     ATM4/0/0     0       34      REMOVED
ATM4/1/0     0       34       PVC     ATM4/0/1     0       34      REMOVED
```

Note The well known connections for signaling, ILMI, and PNNI are automatically setup and reconfigured.

The previously configured cross-connections will be reestablished if the bandwidth requirements are the same. Table 4-2 lists the port adapter module that can be hot-swapped without reconfiguration of the connections between interfaces. For example, a 155 single-mode PAM can be hot-swapped with a 155 multimode PAM and the connections will be reestablished as described in the section “Replace a PAM with the Same PAM Type.”

Table 4-2 PAM Hot Swap Reconfiguration Matrix

Port Adapter Module Type	155 UTP	155 SM	155 MM	DS-3	E3	622 SM
155 UTP	No reconfig	No reconfig	No reconfig	Reconfig	Reconfig	Reconfig
155 SM	No reconfig	No reconfig	No reconfig	Reconfig	Reconfig	Reconfig
155 MM	No reconfig	No reconfig	No reconfig	Reconfig	Reconfig	Reconfig
DS-3	Reconfig	Reconfig	Reconfig	No reconfig	Reconfig	Reconfig
E-3	Reconfig	Reconfig	Reconfig	Reconfig	No reconfig	Reconfig
622 SM	Reconfig	Reconfig	Reconfig	Reconfig	Reconfig	No reconfig

Use the **no atm pvc** command to remove existing connections after hot-swapping a PAM and replacing it with a different type or speed PAM if new connections to the same VPI/VCI are desired, as shown Figure 4-7.

Figure 4-7 no atm pvc Example

```
Switch#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#int atm 4/1/0
Switch(config-if)#atm pvc 0 33 interface atm 4/0/0 0 34
%connection creation fails: vpi/vci has been used by other connections
Switch(config-if)#no atm pvc 0 33
Switch(config-if)#atm pvc 0 33 interface atm 4/0/0 0 34
Switch(config-if)#
```

After hot-swapping to a new PAM type use the **copy running-config startup-config** to replace the original PAM configuration with the new PAM configuration. Any connections listed as removed will not be stored in NVRAM.

Configure the Network Routing

The default software image for the LightStream 1010 contains only the IISP routing protocol. This is suitable for small networks that do not require the sophistication of the PNNI protocols. A separate orderable image contains both PNNI and IISP protocols. The PNNI protocol provides the route dissemination mechanism for complete plug-and-play capability.

The section “Configure ATM Static Routes for IISP or PNNI” describe modifications that may be made to the default PNNI or IISP routing configurations.

For a detailed descriptions of these routing protocols see the section “ATM Routing” in the chapter “LightStream 1010 Product Overview” and the chapters “Configuring ILMI” and “Configuring PNNI” for detailed configuration information.

Configure ATM Static Routes for IISP or PNNI

Use the **atm route** command to configure a static route. Static route configuration allows ATM call setup requests to be forwarded on a specific interface if the addresses match a configured address prefix.

Note An interface must be UNI or IISP to be configured with static route. Static routes configured as on PNNI interfaces will default as down.

Figure 4-8 is an example of the **atm route** command configuring the 13-byte-peer-group-prefix = 47.0091.8100.567.0000.0ca7.ce01 at interface 3/0/0:

Figure 4-8 atm route Command Example

```
Switch(config)#atm route 47.0091.8100.567.0000.0ca7.ce01 atm 3/0/0
Switch(config)#
```

Configure the System Information

Although not required, several system parameters should be set as part of the initial system configuration. To set the system parameters, perform the following tasks in EXEC mode:

Task	Command
Set the system clock.	**clock set** ***day_of_week mm/dd/yy hh:mm:ss***
At the privileged EXEC prompt, enter configuration mode from the terminal.	**configure**[1] [**terminal**]
Set the system name.	**hostname** *name_string*

1. This command is documented in the *LightStream 1010 ATM Switch Command Reference* publication.

Syntax Description

hh:mm:ss—Current time in hours (military format), minutes, and seconds.

day —Current day (by date) in the month.

month—Current month (by name).

year—Current year (no abbreviation).

name_string—New case sensitive host name for the network server.

Configure SNMP Management

Simple Network Management Protocol (SNMP), an application-layer protocol, facilitates the exchange of management information bases (MIBs) between network devices. SNMP community strings authenticate access to the MIB and function as embedded “passwords.”

SNMP may be manually configured using the following defaults:

- community string = public
- access string = read only
- snmp trap = enable

For definitions of all commands discussed in this chapter, refer to the publication *LightStream 1010 ATM Switch Command Reference.*

The Simple Network Management Protocol (SNMP) system consists of three parts: an SNMP manager, an SNMP agent, and a Management Information Base (MIB). SNMP is an application-layer protocol that allows SNMP manager and agent stations to communicate. SNMP provides a message format for sending information between an SNMP manager and an SNMP agent. The SNMP manager can be part of a Network Management System (NMS), such as CiscoWorks.

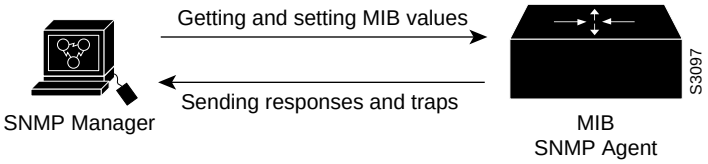
The agent and MIB reside on the switch. In configuring SNMP on the switch, you define the relationship between the manager and the agent.

The SNMP agent contains MIB variables whose values the SNMP manager can request or change. A manager can get a value from an agent or store a value into that agent.The agent gathers data from the MIB, the repository for information about device parameters and network data. The agent can also respond to a manager's requests to get or set data.

An agent can also send unsolicited traps to the manager. Traps are messages alerting the SNMP manager to a condition on the network. Traps can indicate improper user authentication, restarts, link status (up or down), closing of a TCP connection, or loss of connection to a neighbor switch.

Figure 4-9 illustrates the communications relationship between the SNMP manager and agent. It shows that a manager can send the agent requests to get and set MIB values. The agent can respond to these requests. Independent of this interaction, the agent can send unsolicited traps to the manager notifying the manager of network conditions.

Figure 4-9 Communication between an SNMP Agent and Manager



Cisco supports the SNMP Version 1 protocol, referred to as SNMPv1, and the SNMP Version 2 protocol, referred to as SNMPv2. Our implementation of SNMP supports all MIB II variables (as described in RFC 1213) and SNMP traps (as described in RFC 1215). Cisco also supports the definition of management information described in RFCs 1155, 1157, and 1213, and supports some or all variables in the MIBs described in the following RFCs: 1156, 1212, 1231, 1243, 1285, 1286, 1315, 1381, 1382, 1398, 1447, 1450, and 1285 (FDDI).

RFC 1447, "SNMPv2 Party MIB" (April 1993), describes the managed objects that correspond to the properties associated with SNMPv2 parties, SNMPv2 contexts, and access control policies, as defined by the SNMPv2 Administrative Model. RFC 1450, "SNMPv2 MIB," (April 1993) describes the managed objects that instrument the behavior of an SNMPv2 implementation. Cisco supports the MIB variables as required by the conformance clauses specified in these MIBs.

Cisco also provides its own MIB with every system. The Cisco MIB provides a new chassis MIB variable that enables the SNMP manager to gather data on system card descriptions, serial numbers, hardware and software revision levels, and slot locations.

See the *Cisco Management Information Base (MIB) User Quick Reference* for a detailed description of each Cisco MIB variable and SNMP trap.

Although SNMPv2 offers more robust support than SNMPv1, Cisco continues to support SNMPv1. This is because not all management stations have migrated to SNMPv2 and you must configure the relationship between the agent and the manager to use the version of SNMP supported by the management station.

SNMPv1 offers a community-based form of security defined through an IP address access control list and password. SNMPv2 offers richer security configured through an access policy that defines the relationship between a single manager and agent. SNMPv2 security includes message authentication support using the Message Digest (MD5) algorithm, but because of the Data Encryption Standard (DES) export restrictions, it does not include encryption support through DES. SNMPv2 security provides data origin authentication, ensures data integrity, and protects against message stream modification.

In addition to enhanced security, SNMPv2 support includes a bulk retrieval mechanism and more detailed error message reporting to management stations. The bulk retrieval mechanism supports the retrieval of tables and large quantities of information, minimizing the number of round-trips required.

The SNMPv2 improved error handling support includes expanded error codes that distinguish different kinds of error conditions; these conditions are reported through a single error code in SNMPv1. Error return codes now report the error type. Three kinds of exceptions are also reported: no such object exceptions, no such instance exceptions, and end of MIB view exceptions.

No specific command enables SNMP. The first **snmp-server** command that you enter enables both versions of SNMP.

To configure SNMP support, perform the tasks in one of the following sections:

- Configure for Both SNMPv1 and SNMPv2
- Configure SNMPv2 Support
- Configure SNMPv1 Support

To configure relationship between the agent and the manager on the switch, you need to know the version of the SNMP protocol that the management station supports. An agent can communicate with multiple managers; for this reason, you can configure the switch to support communications with one management station using the SNMPv1 protocol and another using the SNMPv2 protocol.

Configure for Both SNMPv1 and SNMPv2

You can perform tasks in the following sections to configure support for both SNMPv1 and SNMPv2 on the switch:

- Enable the SNMP Agent Shutdown Mechanism
- Establish the Contact, Location, and Serial Number of the SNMP Agent
- Define the Maximum SNMP Agent Packet Size
- Monitor SNMP Status
- Disable the SNMP Agent

Enable the SNMP Agent Shutdown Mechanism

Using SNMP packets, a network management tool can send messages to users on virtual terminals and the console. This facility operates in a similar fashion to the EXEC **send** command; however, the SNMP request that causes the message to be issued to the users also specifies the action to be taken after the message is delivered. One possible action is a shutdown request. After a system is shut down, typically it is reloaded. Because the ability to cause a reload from the network is a

powerful feature, it is protected by the **snmp-server system-shutdown** global configuration command. If you do not issue this command, the shutdown mechanism is not enabled. To enable the SNMP agent shutdown mechanism, perform the following task:

Task	Command
Use the SNMP message reload feature and request a system shutdown message.	**snmp-server system-shutdown**

To understand how to use this feature with SNMP requests, read the document *mib.txt* available by anonymous FTP from *ftp.cisco.com.*

Establish the Contact, Location, and Serial Number of the SNMP Agent

You can set the system contact, location, and serial number of the SNMP agent so that these descriptions can be accessed through the configuration file. To do so, perform one or more of the following tasks in global configuration mode:

Task	Command
Set the system contact string.	**snmp-server contact** *text*
Set the system location string.	**snmp-server location** *text*
Set the system serial number.	**snmp-server chassis-id** *text*

Define the Maximum SNMP Agent Packet Size

You can set the maximum packet size permitted when the SNMP agent is receiving a request or generating a reply. To do so, perform the following task in global configuration mode:

Task	Command
Establish the maximum packet size.	**snmp-server packetsize** *byte-count*

Monitor SNMP Status

To monitor SNMP input and output statistics, including the number of illegal community string entries, errors, and requested variables, complete the following task in EXEC mode:

Task	Command
Monitor SNMP status.	**show snmp**

Disable the SNMP Agent

To disable both versions of SNMP (SNMPv1 and SNMPv2) concurrently, perform the following task in global configuration mode:

Task	Command
Disable SNMP agent operation.	**no snmp-server**

Configure SNMPv2 Support

SNMPv2 security requires that you create an access policy that defines the relationship between a manager and the agent. For each management station with the agent communicates, you must create a separate access policy. Creating an access policy is a multiple-task process:

Step 1 Define a view to identify the objects that can be seen, if you do not want to use one of the standard predefined views.

Step 2 Define a context to identify the object resources that can be acted on.

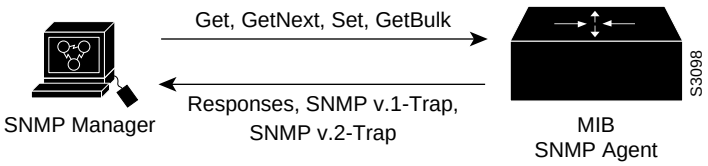
Step 3 Define a party for both the manager and the agent to identify them.

Step 4 Using the definitions created in the previous tasks, configure the access policy that characterizes the communications that can occur between the manager and the agent. The privileges that you define for the access policy depend on whether the agent is defined as the source or the destination. For example:

- When the agent party is defined as the destination in an access policy, the access policy privileges define the management operations that the agent will accept from the manager and perform in relation to the object resources.
- When the agent party is defined as the source in an access policy, the access policy privileges define the responses and traps that the agent can send to the manager.

Figure 4-10 shows the information exchanged between the manager and the agent. The top arrow, leading from the manager to the agent, shows the types of requests the manager can send to the agent. The bottom arrow, leading from the agent to the manager, shows the kind of information that the agent can send to the manager. Note that the agent sends trap messages to the manager in response to certain network conditions; trap messages are unsolicited and are not related to the request/response communication exchange between the manager and the agent that occurs in relation to MIB variables. For any given manager and agent relationship, the privileges defined in the access policy constrain communications to a specific set of operations.

Figure 4-10 Flow of Management Operations Requests, Responses, and Traps between the Manager and the Agent



You must create access policies for each new agent that is installed. You also must create access policies on an agent when new management stations with which the agent will communicate are installed. Moreover, every time a network address changes on a management station, you must reconfigure the access policy to reflect the new information for the management station.

Because the process of creating an access policy is complex and must be performed many times, SNMPv2 offers a single-step method that relies on an accepted set of conventions called the *simplified security conventions*. You can configure security using this simplified method only if both the agent and the manager support it and consent to use it. The simplified method offers ease of use, but at the cost of forfeiting control over some values that can be configured if you create an access policy.

If you use the simplified security conventions method, the SNMPv2 implementation assumes default values that it determines internally for required information that you cannot provide through the command interface. To use the simplified method, you enter one command supplying a user ID, and optionally, the name of a view, access rights, and a password. The SNMPv2 implementation on the switch derives most of the configuration information from other values.

This section describes each task that you must perform to configure an access policy. Then it addresses the alternative method and describes the task of configuring the user ID for the simplified security conventions method.

To configure support for SNMv2 on the switch, you perform the following tasks:

- Create or Modify an SNMP View Record
- Create or Modify an SNMP Context Record
- Create or Modify an SNMPv2 Party Record
- Create an SNMPv2 Access Policy
- Create or Modify an SNMPv2 Simplified Security Context Record
- Define SNMPv2 Trap Operations

After you create a record, you can modify the record's contents, changing one or more of the record values. To do this, you issue the command again, naming the record that you created originally. You must fully specify the record values, including the argument values to remain unchanged.

Create or Modify an SNMP View Record

To create or modify an SNMP view record, perform the following task in global configuration mode:

Task	Command
Create or modify a view record.	**snmp-server view** *view-name oid-tree* {**included** | **excluded**}

To remove a view record, use the **no snmp-server view** command.

Create or Modify an SNMP Context Record

To create or modify an SNMP context record, perform the following task in global configuration mode:

Task	Command
Create or modify a context record.	**snmp-server context** *context-name context-oid view-name*

To remove a context entry, use the **no snmp-server context** command. Specify only the name of the context. The name identifies the context to be deleted.

Create or Modify an SNMPv2 Party Record

To create or modify an SNMPv2 party record, perform the following task in global configuration mode:

Task	Command
Create or modify a party record.	**snmp-server party** *party-name party-oid* [*protocol-address*] [**packetsize** *size*] [**local** | **remote**] [**authentication md5** *key* [**clock** *clock*] [**lifetime** *lifetime*]

To remove a party record, use the **no snmp-server party** command.

Create an SNMPv2 Access Policy

To create or modify an SNMPv2 access policy, perform the following task in global configuration mode:

Task	Command
Create or modify an access policy.	**snmp-server access-policy** *destination-party source-party context privileges*

To remove an SNMPv2 access-policy, use the **no snmp-server access-policy** command. Specify all three arguments to correctly identify the access policy to be deleted. A difference of one value constitutes a unique access policy entry.

Create or Modify an SNMPv2 Simplified Security Context Record

To create or modify a simplified security context record, perform the following task in global configuration mode:

Task	Command
Create or modify a context record.	**snmp-server userid** *user-id* [**view** *view-name*] [**ro** | **rw**] [**password** *password*]

To remove a simplified security context record, use the **no snmp-server userid** command.

Note You may choose to use the same user ID and password across several machines. Because other values are derived internally from the agent's IP address, these configurations are unique.

Define SNMPv2 Trap Operations

A trap is an unsolicited message sent by an SNMP agent to an SNMP manager indicating that some event has occurred. The SNMP trap operations allow you to configure the switch to send information to a network management application when a particular event occurs. You can specify the following features for SNMPv2 agent trap operations:

- Source interface
- Recipient of the trap message
- Trap message authentication

- Retransmission interval
- Message (packet) queue length for each trap host

To define the recipient of the trap message, you configure a party record for the manager, including the protocol address, and specify the party record as the destination party for the **snmp-server access policy** command. To define traps for the agent to send to the manager, perform one or more of the following tasks in global configuration mode:

Task	Command
Specify the source interface (and hence IP address) of the trap message.	**snmp-server trap-source** *interface*
Specify the access policy that defines the traps that the agent can send to the manager.	**snmp-server access-policy** *destination-party source-party context privileges*
Establish trap message authentication.	**snmp-server trap-authentication** [**snmpv1** | **snmpv2**]
Define how often to resend trap messages on the retransmission queue.	**snmp-server trap-timeout** *seconds*
Establish the message queue length for each trap host.	**snmp-server queue-length** *length*

Configure SNMPv1 Support

If the manager supports only the SNMPv1 protocol, you must configure the relationship between the manager and the agent using SNMPv1 support. You can use either of two methods to configure access to the agent. There are trade-offs involved in choosing one method over the other. The methods differ in the following ways:

- Using the **snmp-server community** command, you specify a string, and, optionally, an access list. The string is used as a password. The access list identifies the IP addresses of systems on which SNMPv1 managers reside that might use the community string to gain access to the SNMPv1 agent. You cannot restrict the MIB view using this method.
- Using an access policy, you can specify a password-like string and you can impose a restricted MIB view, but you cannot specify an access list to identify the IP addresses of managers that may access the agent. An SNMPv1 access policy is similar to an SNMPv2 access policy.

To configure support for SNMPv1 on the switch, you perform tasks in the following sections:

- Create or Modify Access Control for an SNMPv1 Community
- Create or Modify an SNMP View Record
- Create or Modify an SNMP Context Record
- Create or Modify a Party Record
- Configure an SNMP Access Policy
- Define SNMP Trap Operations for SNMPv1

Create or Modify Access Control for an SNMPv1 Community

You can configure a community string, which acts like a password, to permit access to the agent on the switch. Optionally, you can associate a list of IP addresses with that community string to permit only managers with these IP addresses to use the string.

To configure a community string, perform the following task in global configuration mode:

Task	Command
Define the community access string.	**snmp-server community** *string* [**ro** | **rw**] [*access-list number*]

You can configure one or more community strings. To remove a specific community string, use the **no snmp-server community** command.

Create or Modify an SNMP View Record

To create or modify an SNMP view record, perform the following task in global configuration mode:

Task	Command
Create or modify a view record to be used for a context record.	**snmp-server view** *view-name oid-tree* {**included** | **excluded**}

To remove a view record, use the **no snmp-server view** command.

Create or Modify an SNMP Context Record

To create or modify an SNMP context record, perform the following task in global configuration mode:

Task	Command
Create or modify a context record to be used for a party record.	**snmp-server context** *context-name context-oid view-name*

To remove a context entry, use the **no snmp-server context** command. Specify only the name of the context. The name identifies the context to be deleted.

Create or Modify a Party Record

To create or modify an SNMPv1 party record to be used in an access policy, perform the following task in global configuration mode:

Task	Command
Create or modify a party record.	**snmp-server party** *party-name party-oid* [*protocol-address*] [**packetsize** *size*] [**local** | **remote**] [**authentication snmpv1** *string*]

To remove a party record, use the **no snmp-server party** command.

Configure an SNMP Access Policy

To configure an access policy, you specify the SNMPv1 proxy for which you configured the party record as both the destination party and the source party. To configure an access policy, perform the following task in global configuration mode:

Task	Command
Create an access policy.	**snmp-server access-policy** *destination-party source-party context privileges*

To remove an SNMP access policy, use the **no snmp-server access-policy** command. Specify all three arguments to correctly identify the access policy to be deleted. A difference of one value constitutes a unique access policy entry.

Define SNMP Trap Operations for SNMPv1

The SNMP trap operations allow a system administrator to configure the agent switch to send information to a manager when a particular event occurs. You can specify the following features for SNMP server trap operations:

- Source interface
- Recipient
- Trap message authentication
- Retransmission interval
- Define the message (packet) queue length for each trap host

Perform the following tasks in global configuration mode to define traps for the agent to send to the specified manager:

Task	Command
Specify the source interface (and hence IP address) of the trap message.	**snmp-server trap-source** *interface*
Specify the recipient of the trap message.	**snmp-server host** *address community-string* [**snmp**] [**tty**]
Establish trap message authentication.	**snmp-server trap-authentication snmpv1**
Define how often to resend trap messages on the retransmission queue.	**snmp-server trap-timeout** *seconds*
Establish the message queue length for each trap host.	**snmp-server queue-length** *length*

Store the Configuration

When autoconfiguration and any manual configurations are complete you should copy the configuration into nonvolatile random-access memory (NVRAM). If you should power off your LightStream 1010 prior to saving the configuration in NVRAM, all manual configuration changes will be lost. Figure 4-11 is an example of the **copy running-config** command.

Figure 4-11 Storing Configuration in NVRAM Example

```
Switch#copy running-config startup-config
Building configuration...
[OK]
Switch#
```

Test the Configuration

When you have finished configuring the LightStream 1010 ATM switch, you can use the following commands to confirm the hardware, software, and interface configuration:

- Use show hardware to Confirm Hardware Configuration
- Use show version to Confirm Software
- Use show interface ethernet to Confirm Ethernet Configuration
- Use show atm address Command to Confirm ATM Address
- Use ping to Test the Ethernet Connection
- Use ping atm to Confirm the ATM Connections
- Use show atm interface to Confirm ATM Interface Configuration
- Use show atm status to Confirm Interface Status
- Use show atm vc to Confirm Virtual Connection
- Use show running-config to Confirm Configuration
- Use show startup-config to Confirm Saved Configuration

Use show hardware to Confirm Hardware Configuration

Use the **show hardware** command to confirm the correct hardware installation. Figure 4-12 provides an example of the show hardware command:

Figure 4-12 show hardware Command Example

```
Switch#show hardware

LS1010 named Switch, Date: 12:50:30 UTC Wed Apr 24 1996

Slot Ctrlr-Type    Part No.  Rev  Ser No  Mfg Date  RMA No. Hw Vrs  Tst EEP
---- ------------  ---------- -- -------- -------- -------- ------- --- ---
0/0  155UTP PAM    73-1572-02 01 02749041  1/17/96 00-00-00   3.0     0   2
0/1  155MM PAM     73-1496-03 06 02180424  1/16/96 00-00-00   3.0     0   2
1/0  155MM PAM     73-1496-03 06 02180444  1/17/96 00-00-00   3.0     0   2
1/1  155MM PAM     73-1496-03 06 02202228  1/11/96 00-00-00   3.0     0   2
2/0  ATM Swi/Proc  73-1402-02 00 02827677  0/07/13 00-00-00   2.3     0   2

Switch#
```

Use show version to Confirm Software

Use the **show version** command to confirm the correct version and type of LightStream 1010 software is installed and the configuration register. Figure 4-13 is an example of the show version command:

Figure 4-13 show version Command Example

```
Switch#show version
Cisco Internetwork Operating System Software
IOS (tm) PNNI Software (LS1010-WP-M), Version 11.1(4)
Copyright (c) 1986-1996 by cisco Systems, Inc.
Compiled Mon 08-Jul-96 05:13 by
Image text-base: 0x600108D0, data-base: 0x60330000

ROM: System Bootstrap, Version 11.2(4)

Switch uptime is 3 days, 19 hours, 2 minutes
System restarted by reload
System image file is "slot0:ls1010-wp-mz.111-3.005", booted via

cisco ASP (R4600) processor with 16384K bytes of memory.
R4600 processor, Implementation 32, Revision 2.0
Last reset from power-on
1 Ethernet/IEEE 802.3 interface.
16 ATM network interfaces.
125K bytes of non-volatile configuration memory.

8192K bytes of Flash PCMCIA card at slot 0 (Sector size 128K).
8192K bytes of Flash internal SIMM (Sector size 256K).
Configuration register is 0x100

Switch#
```

Use show interface ethernet to Confirm Ethernet Configuration

Use the **show interface ethernet** command to confirm the ethernet interface on the ASP is configured correctly. Figure 4-14 is an example of the show interface ethernet command:

Figure 4-14 show interface ethernet 2/0/0 Command Example

```
Switch#show interface ethernet 2/0/0
Ethernet2/0/0 is up, line protocol is up
  Hardware is SonicT, address is 0000.0ca7.ce00 (bia 0000.0ca7.ce00)
  Internet address is 172.20.40.43 255.255.255.0
  MTU 1500 bytes, BW 10000 Kbit, DLY 1000 usec, rely 255/255, load 1/255
  Encapsulation ARPA, loopback not set, keepalive set (10 sec)
  ARP type: ARPA, ARP Timeout 4:00:00
  Last input 0:00:26, output 0:00:16, output hang never
  Last clearing of "show interface" counters never
  Output queue 0/40, 0 drops; input queue 0/75, 0 drops
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     6021 packets input, 2145763 bytes, 0 no buffer
     Received 6019 broadcasts, 0 runts, 0 giants
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored, 0 abort
     0 input packets with dribble condition detected
     113 packets output, 31148 bytes, 0 underruns
     0 output errors, 0 collisions, 1 interface resets, 0 restarts
     0 output buffer failures, 0 output buffers swapped out
Switch#
```

Use show atm address Command to Confirm ATM Address

Use the **show atm address** command to confirm correct configuration of the ATM address for the LightStream 1010. Figure 4-15 provides an example of the **show atm address** command:

Figure 4-15 show atm address Command Example

```
Switch#show atm address

Switch Address(es):
  47.00918100000000603E5ADB01.00603E5ADB01.00 active

Soft VC Address(es):
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0000.00 ATM0/0/0
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0000.63 ATM0/0/0.99
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0010.00 ATM0/0/1
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0020.00 ATM0/0/2
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0030.00 ATM0/0/3
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.1000.00 ATM0/1/0
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.1010.00 ATM0/1/1
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.1020.00 ATM0/1/2
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.1030.00 ATM0/1/3
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.8000.00 ATM1/0/0
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.8010.00 ATM1/0/1
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.8020.00 ATM1/0/2
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.8030.00 ATM1/0/3
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.9000.00 ATM1/1/0
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.9010.00 ATM1/1/1
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.9020.00 ATM1/1/2
  47.0091.8100.0000.0060.3e5a.db01.4000.0c80.9030.00 ATM1/1/3

ILMI Switch Prefix(es):
  47.0091.8100.0000.0060.3e5a.db01

ILMI Configured Interface Prefix(es):

LECS Address(es):
Switch#
```

Use ping to Test the Ethernet Connection

After you have configured the IP address(es) for the Ethernet interface, test for connectivity between the switch and a host. The host can reside anywhere in your network. To test for Ethernet connectivity, perform the following task:

Task	Command
Test the configuration using the ping command. The ping command sends an echo request to the host specified in the command line.	**ping ip *ip_address***

For example, to test Ethernet connectivity from the switch to a workstation with an IP address of 172.20.40.201, enter the command **ping ip 172.20.40.201**. If the switch receives a response, the following message is displayed:

```
Switch#ping ip 172.20.40.201

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.20.40.201, timeout is 2 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/202/1000 ms
Switch#
```

Use ping atm to Confirm the ATM Connections

Use the **ping atm** command to confirm that the ATM interfaces are configured correctly. Figure 4-16 is an example of the ping atm command:

Figure 4-16 ping atm Command Example

```
Switch#ping atm interface atm 3/0/0 0 5 seg-loopback

Type escape sequence to abort.
Sending Seg-Loopback 5, 53-byte OAM Echoes to a neighbour,timeout is 5 seconds:
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/1/4 ms
Switch#
```

Use show atm interface to Confirm ATM Interface Configuration

Use the **show atm interface** command to confirm the atm interfaces are configured correctly. Figure 4-17 is an example of the show atm interface command:

Figure 4-17 show atm interface Command Example

```
Switch#show atm interface

Interface:      ATM0/0/0        Port-type:    oc3suni
IF Status:      UP              Admin Status: up
Auto-config:    disabled        AutoCfgState: not applicable
IF-Side:        User            IF-type:      IISP
Uni-type:       not applicable  Uni-version:  V3.0
Max-VPI-bits:   8               Max-VCI-bits: 14
Max-VP:         255             Max-VC:       32768
ATM Address for Soft VC: 47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0000.00
Configured virtual links:
  PVCLs SoftVCLs   SVCLs   PVPLs SoftVPLs   SVPLs  Total-Cfgd  Installed-Conns
      3        0       0       2        0       0           5                4
Logical ports(VP-tunnels):     1
Input cells:    200             Output cells: 813
5 minute input rate:             0 bits/sec,       0 cells/sec
5 minute output rate:            0 bits/sec,       0 cells/sec
Input AAL5 pkts: 200, Output AAL5 pkts: 813, AAL5 crc errors: 0


Interface:      ATM0/0/0.99     Port-type:    vp tunnel
```

```
IF Status:      UP              Admin Status: up
Auto-config:    disabled        AutoCfgState: not applicable
IF-Side:        Network         IF-type:      UNI
Uni-type:       Private         Uni-version:  V3.0
Max-VPI-bits:   8               Max-VCI-bits: 14
Max-VP:         0               Max-VC:       32768
ATM Address for Soft VC: 47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0000.63
Configured virtual links:
  PVCLs SoftVCLs   SVCLs  Total-Cfgd  Installed-Conns
      5        0       0           5                5


Interface:      ATM0/0/1        Port-type:    oc3suni
IF Status:      UP              Admin Status: up
Auto-config:    disabled        AutoCfgState: not applicable
IF-Side:        User            IF-type:      IISP
Uni-type:       not applicable  Uni-version:  V3.0
Max-VPI-bits:   8               Max-VCI-bits: 14
Max-VP:         255             Max-VC:       32768
ATM Address for Soft VC: 47.0091.8100.0000.0060.3e5a.db01.4000.0c80.0010.00
Configured virtual links:
  PVCLs SoftVCLs   SVCLs   PVPLs SoftVPLs   SVPLs  Total-Cfgd  Installed-Conns
      3        0       0       0        0       0           3                3
Logical ports(VP-tunnels):     0
Input cells:    814             Output cells: 202
5 minute input rate:             0 bits/sec,       0 cells/sec
 --More--

<Information Deleted>
```

Use show atm status to Confirm Interface Status

Use the **show atm status** command to confirm the status of ATM interfaces. Figure 4-18 is an example of the show atm status command:

Figure 4-18 show atm status Command Example

```
Switch#show atm status
NUMBER OF INSTALLED CONNECTIONS: (P2P=Point to Point, P2MP=Point to MultiPoint)

Type       PVCs  SoftPVCs      SVCs      PVPs  SoftPVPs      SVPs      Total
P2P          18         0         0         0         0         0         18
P2MP          0         0         0         0         0         0          0
                                   TOTAL INSTALLED CONNECTIONS =         18

PER-INTERFACE STATUS SUMMARY AT 14:25:42 UTC Wed Apr 24 1996:
   Interface      IF         Admin  Auto-Cfg    ILMI Addr     SSCOP
     Name       Status      Status    Status    Reg State     State
------------- -------- ------------ -------- ------------ ---------
ATM0/0/0          DOWN     shutdown      n/a          n/a      Idle
ATM0/0/0.99       DOWN     shutdown      n/a          n/a      Idle
ATM0/0/1          DOWN         down      n/a          n/a      Idle
ATM0/0/2            UP           up      n/a          n/a    Active
ATM0/0/3            UP           up     done  UpAndNormal    Active
ATM0/1/0            UP           up     done  UpAndNormal    Active
ATM0/1/1            UP           up     done  UpAndNormal    Active
ATM0/1/2          DOWN         down  waiting          n/a      Idle
ATM0/1/3          DOWN         down  waiting          n/a      Idle
ATM1/0/0            UP           up     done  UpAndNormal    Active
ATM1/0/1          DOWN         down  waiting          n/a      Idle
ATM1/0/2          DOWN         down  waiting          n/a      Idle
```

```
ATM1/0/3            UP           up     done  UpAndNormal    Active
ATM1/1/0          DOWN         down  waiting          n/a      Idle
ATM1/1/1          DOWN         down  waiting          n/a      Idle
ATM1/1/2          DOWN         down  waiting          n/a      Idle
ATM1/1/3          DOWN         down  waiting          n/a      Idle
ATM2/0/0            UP           up      n/a  UpAndNormal      Idle
Switch#
```

Use show atm vc to Confirm Virtual Connection

Use the **show atm vc** command to confirm the status of ATM virtual interfaces. Figure 4-19 is an example of the show atm vc command:

Figure 4-19 show atm vc Command Example

```
Switch#show atm vc
Interface    VPI     VCI     Type   X-Interface  X-VPI   X-VCI   Status
ATM0/0/0     0       5        PVC     ATM2/0/0     0       32      DOWN
ATM0/0/0     0       16       PVC     ATM2/0/0     0       33      DOWN
ATM0/0/0     0       18       PVC     ATM2/0/0     0       34      DOWN
ATM0/0/0.99  99      3        PVC     ATM2/0/0     0       83      DOWN
ATM0/0/0.99  99      4        PVC     ATM2/0/0     0       84      DOWN
ATM0/0/0.99  99      5        PVC     ATM2/0/0     0       80      DOWN
ATM0/0/0.99  99      16       PVC     ATM2/0/0     0       81      DOWN
ATM0/0/0.99  99      18       PVC     ATM2/0/0     0       82      DOWN
ATM0/0/1     0       5        PVC     ATM2/0/0     0       35      DOWN
ATM0/0/1     0       16       PVC     ATM2/0/0     0       36      DOWN
ATM0/0/1     0       18       PVC     ATM2/0/0     0       37      DOWN
ATM0/0/2     0       5        PVC     ATM2/0/0     0       38      UP
ATM0/0/2     0       16       PVC     ATM2/0/0     0       39      UP
ATM0/0/2     0       18       PVC     ATM2/0/0     0       40      UP
ATM0/0/3     0       5        PVC     ATM2/0/0     0       41      UP
ATM0/0/3     0       16       PVC     ATM2/0/0     0       42      UP
ATM0/0/3     0       18       PVC     ATM2/0/0     0       43      UP
ATM0/1/0     0       5        PVC     ATM2/0/0     0       44      UP
ATM0/1/0     0       16       PVC     ATM2/0/0     0       45      UP
ATM0/1/0     0       18       PVC     ATM2/0/0     0       46      UP
ATM0/1/1     0       5        PVC     ATM2/0/0     0       47      UP
ATM0/1/1     0       16       PVC     ATM2/0/0     0       48      UP
 --More--
```

Use show running-config to Confirm Configuration

Use the **show running-configuration** command to confirm the configuration being used is configured correctly. Figure 4-20 is an example of the write terminal command:

Figure 4-20 show running-configuration Command Example

```
Switch#show  running-config
Building configuration...

Current configuration:
!
version 11.1
no service pad
```

```
service udp-small-servers
service tcp-small-servers
!
hostname Switch
!
boot system flash slot0:rhino/ls1010-wi-m_1.083.bin.Z
!
atm over-subscription-factor 16
atm service-category-limit cbr 3000
atm qos uni3-default  cbr max-cell-loss-ratio 12
atm address 47.0091.8100.0000.0060.3e5a.db01.0060.3e5a.db01.00
!
interface ATM0/0/0
 no keepalive
 shutdown
 no atm auto-configuration
 no atm address-registration
 no atm ilmi-enable
 no atm ilmi-lecs-implied
 atm iisp side user
 atm pvp 99

<Information Deleated>

interface ATM1/1/3
 no keepalive
!
interface ATM2/0/0
 mtu 1500
 no ip address
 no ip route-cache
 no keepalive
 atm maxvp-number 0
 lane client ethernet mis
 lane client-atm-address ...0800200C1001**
 lane pvc 100 55.00550055005500550055.00000C0425C2.00
!
interface Ethernet2/0/0
 ip address 172.20.40.93 255.255.255.0
 no ip route-cache
!
interface Ethernet2/0/0.100
 no ip route-cache
!
ip default-gateway 172.20.40.201
no ip classless
atm route default ATM0/0/0
atm route 47.0091.8100.5670.ca7c.e01... ATM2/0/0
atm route 47.0091.8100.0000.0000.0ca7.ce01... ATM0/0/0
!
line con 0
 exec-timeout 0 0
 vacant-message ^C hello ^C
line aux 0
 transport input all
line vty 0 4
 login
!
end

Switch#
```

Use show startup-config to Confirm Saved Configuration

Use the **show configuration** command to confirm the configuration saved in NVRAM is configured correctly. Figure 4-21 is an example of the show configuration command:

Figure 4-21 show startup-config Command Example

```
Switch#show startup-config

Switch#show startup-config
Using 2519 out of 129016 bytes
!
version 11.1
no service pad
service udp-small-servers
service tcp-small-servers
!
hostname Switch
!
boot system flash slot0:rhino/ls1010-wi-m_1.083.bin.Z
!
ip rcmd remote-username dplatz
atm over-subscription-factor 16
atm service-category-limit cbr 3000
atm qos uni3-default  cbr max-cell-loss-ratio 12
atm lecs-address 47.0091.0000.0000.0000.0000.0000.0000.0000.0000.00
atm address 47.0091.8100.0000.0060.3e5a.db01.0060.3e5a.db01.00
!
interface ATM0/0/0
 no keepalive
 map-group atm-1
 no atm auto-configuration
 no atm address-registration
 no atm ilmi-enable
 no atm ilmi-lecs-implied
 atm iisp side user
 atm pvp 99
!
interface ATM0/0/0.99 point-to-point
 no atm auto-configuration
 no atm address-registration
 no atm ilmi-enable
 no atm ilmi-lecs-implied
 atm maxvp-number 0
!
interface ATM0/0/1
 no keepalive
 no atm auto-configuration
 no atm address-registration
 no atm ilmi-enable
 no atm ilmi-lecs-implied
 atm iisp side user
!
interface ATM0/0/2
 no keepalive
 no atm auto-configuration
 --More--

<Information Deleted>

ip default-gateway 172.20.40.201
no ip classless
```

```
!
map-list atm
!
map-list atm_1
!
map-list atm-1
 ip 10.0.0.2 atm-vc 200 broadcast
!
map-list yyy
 ip 1.1.1.1 atm-vc 200
 ip 1.1.1.2 atm-vc 200
!
map-list zzz
!
map-list atm1
!
map-class atm atm-class
atm route default ATM0/0/0
atm route 47.0091.8100.5670.ca7c.e01... ATM2/0/0
atm route 47.0091.8100.0000.0000.0ca7.ce01... ATM0/0/0
!
line con 0
 exec-timeout 0 0
 vacant-message ^C hello ^C
line aux 0
 transport input all
line vty 0 4
 login
!
end

Switch#
```