APPENDIX H

Configuring ATM Features for the LightStream Switch

This chapter provides procedures for using CiscoView to configure Light Stream Switches for Asynchronous Transfer Mode (ATM). For ATM Lane Emulation (LANE) configuration information for Catalyst switches, refer to Appendix G, "Configuring ATM LANE for Catalyst Switches."

ATM features for the LightStream switches are described in the following sections, which contain a variety of features used for ATM configuration:

- Managing ATM Device Features
- Managing ATM Port Features

Managing ATM Device Features

The ATM device features provide access to the following options:

- Resource Management (Global)
- ATM OAM
- ATM RMON
- ATM Accounting
- ATM Signaling (Global)
- ATM Signaling Diagnosis
- PNNI (Global)
- ILMI (Global)

To start the ATM Feature application, select **ATM Features** from the menu bar.

Timesaver To display information for any category, select the category from the pull-down menu next to the CATEGORY label. Within each ATM device feature, change the category to access different management features.

Tip Where windows display optional fields, you can enter a value, or you can leave the field blank so that the device automatically generates the value.

Note For additional information on the fields in the windows, click **Help** to access the CiscoView online help.

Resource Management (Global)

The Resource Management (Global) category allows you to manage critical resources in an ATM network, such as buffer space and trunk bandwidth. When the Resource Management (Global) category is selected, the ATM RM Switch Configuration window is displayed.

The following subcategories are available:

- ATM RM Switch Configuration
- ATM RM Queue
- ATM RM Default UNI3 QoS
- ATM Traffic Descriptor
- ATM RM Threshold Group
- ATM RM Threshold Group Service
- ATM RM Service Class
- ATM RM Service Class on Interface

ATM RM Switch

When you select the ATM RM Switch Configuration category, the ATM RM Switch Configuration window opens. This allows you to display or modify available bit rate (ABR) and unspecified bit rate (UBR) configuration information. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hints for Modifying the ATM RM Switch Configuration

When modifying fields, consider the following:

1. When setting the Set the Over-Subscription Factor field, in general, the larger the value, the larger the queue size.
2. When setting the ABR Mode field, consider the following:
    - *relative rate* sets the congestion notification to be received from outside the switch.
    - *EFCI* sets the congestion notification in the headers of forward cells, which are turned around at the destination end system and sent back to the source end system.
    - *both* sets the congestion notification to both the relative rate and EFCI congestion notification types for ABR connections.
3. The default for the Set the Sustained Cell Rate Margin Factor field is 1%.

ATM RM Queue

When you select the ATM RM Queue category, the ATM RM Queue window allows you to display or modify output queue traffic information. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hint for Modifying the ATM RM Queue

When setting the Set the Output Queue Limit field, the output queue limit is 65,535 cells of all priorities combined.

ATM RM Default UNI3 QoS

When you select the ATM RM Default UNI3 QoS category, the ATM RM Default User-Network Interface 3 (UNI3) Quality of Service (QoS) window allows you to display or modify the default QoS information. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hints for Modifying the ATM RM Default UNI3 QoS

When modifying fields, consider the following:

- When setting the Set the Default QoS Max Cell Transfer Delay value, the value is entered in microseconds.
- When setting the Set the Default QoS Cell Loss Ratio for CLP01 value, the value is entered in negative powers of 10.

ATM Traffic Descriptor

When you select the ATM Traffic Descriptor category, the ATM Traffic Descriptor window displays traffic descriptor information. To create a new traffic descriptor, click **Create,** enter values in the fields, and click **Apply**.

Hints for Creating an ATM Traffic Descriptor

When defining the fields, consider the following:

- Enter a unique number in the Set the Descriptor Index field to identify this row in the ATM Traffic Descriptor parameter table.
- The Set the Peak Cell Rate (PCR) value must be entered in kbps.

ATM RM Threshold Group

When you select the ATM RM Threshold Group category, the ATM RM Threshold Group window allows you to display or modify the threshold group information. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hints for Modifying the ATM RM Threshold Group

When defining fields, consider the following:

- The largest allowable Set the Max Size value is 65535.
- Valid Set the Max Queue Size value, valid values are 32 to 16368. The value entered cannot be smaller than the Queue Minimum Size.
- Valid Set the Min Queue Size values are 32 to 16368. The value entered cannot be larger than the Queue Maximum Size.
- The Set the CLP/EPD Threshold (%) value must be entered as a percentage of capacity. Setting this value to 100 effectively turns off the threshold.
- The Set the EFCI/ABR-RR Mark Threshold value is entered as a percentage of capacity. Setting this value to 100 effectively turns off the threshold.

ATM RM Threshold Group Service

When you select the ATM RM Threshold Group Service category, the ATM RM Threshold Group Service window allows you to display or change the threshold group to which VC/VP queues are assigned. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

ATM RM Service Class

When you select the ATM RM Service Class category, the ATM Service Class window displays service class information on this interface.

ATM RM Service Class on Interface

When you select the ATM RM Service Class on Interface category, the ATM Service Class on Interface window displays the service classes on interfaces.

ATM OAM

The ATM OAM category displays OAM Loopback Ping table information for end-to-end or segment connections. When the ATM OAM category is selected, the OAM Ping(end2end) window is displayed.

The following subcategories are available:

- OAM Ping (end2end)
- OAM Ping (segment)

OAM Ping (end2end)

If you select the ATM OAM category, the default OAM Ping(end2end) window displays OAM Loopback Ping table information for end-to-end connections.

Hint for Creating/Modifying an OAM Ping(end2end) Entry

Enter a unique identifier for the Ping SN value in the OAM Loopback Ping table.

OAM Ping (segment)

If you select the OAM Ping (segment) category, the default OAM Ping(segment) window displays OAM Loopback Ping table information for segment connections.

Hints for Creating/Modifying an OAM Ping(segment) Entry

When defining the fields, consider the following:

- Enter a unique identifier for the Ping SN value in the OAM Loopback Ping table.
- The Row Status value is for the row status of the selected table entry.

ATM RMON

The ATM RMON feature allows you to monitor network traffic for reasons such as fault monitoring or capacity planning. The ATM RMON feature is an extension of an existing, well-known RMON standard and provides high-level per-host and per-conversation statistics in a standards-track MIB similar to the following existing RMON MIBs:

- RMON-1 MIB—RFC 1757
- RMON-2 MIB—RFC 2021 and 2074

The ATM-RMON counter uses the per-VC counters already maintained in the hardware and polled by software. The ATM RMON agent can report cell traffic statistics by monitoring connection management activity. At connection setup and release time, some ATM-RMON bookkeeping code is executed. The amount of information varies, depending on the ATM RMON configuration. The bookkeeping capability significantly reduces the CPU requirements for ATM-RMON and allows statistics to be collected on many or all switch ports at once.

Note The ATM-RMON agent uses the 64-bit version of each cell counter if 64-bit counter support is present in the SNMP master-agent library.

When the ATM RMON category is selected, the Data Collection Group window is displayed.

The following subcategories are available:

- Data Collection Group
- Data Collection Group on Interface
- Enable/Disable ATM RMON
- Total Traffic
- In HostTraffic
- Out Host Traffic
- Source Matrix Traffic
- Destination Matrix Traffic

Data Collection Group

Previously, RMON allowed collection of connection information on a per-interface basis only. ATM RMON allows a group of ports to be configured as an aggregate. The port select group defines this *collection unit*. For example, agent 1 can have a port selection group 1 that is composed of ports.

An active port select group must be defined before any data collection can actually begin. You can use the command-line interface (CLI) and SNMP modules to configure and access port select group structures.

Note Use the **atm rmon portselgrp** command to configure an RMON port selection group. See the *LightStream 1010 ATM Switch Software Configuration Guide*, Chapter 14, for more information about this command.

When you select the ATM RMON category, the Data Collection Group window displays the ATM RMON collection group information defined on the device.

Hints for Creating/Modifying a Data Group Collection Entry

When defining the fields, consider the following:

- Enter a unique index number for the Group ID value.
- Leaving the Max Host Entries field blank means that as many entries as possible will be created.
- Leaving the Max Matrix Entries field blank means that as many entries as possible will be created.
- The Matrix Priority values are 1 (low), 2 (normal), or 3 (high); the default is 2.
- The Matrix Address Scope values are 1 (match prefix), 2 (match prefix and ESI), or 3 (entire 20-byte address).

Data Collection Group on Interface

If you select the Data Collection Group on Interface category, the Data Collection Group on Interface window displays the ATM RMON collection group information defined on each port.

Hint for Creating/Modifying a Data Collection Group on Interface Entry

When setting the Group ID value, enter a unique index number for this collection group.

ATM RMON Configuration

To display the ATM RMON configuration, enter the following commands in user EXEC mode:

Command	Task
show running-config	Display the ATM RMON configuration.

Enable/Disable ATM RMON

When you select the Enabling/Disabling ATM RMON category, the Enable/Disable ATM RMON window is displayed. This allows you to enable or disable the ATM RMON feature by selecting active or inactive. To modify the configuration, make a selection then click **Modify**.

If you disable ATM RMO, the configuration remains but becomes inactive (similar to using the **shutdown** command on an interface).

Total Traffic

When you select the Total Traffic category, the Total Traffic window displays the total traffic statistics information for each ATM RMON group.

In Host Traffic

When you select the In Host Traffic category, the In Host Traffic window opens. The In Host Traffic window displays the incoming host traffic statistics information for each ATM RMON group.

Out Host Traffic

When you select the Out Host Traffic category, the Out Host Traffic window displays the outgoing host traffic statistics information for each ATM RMON group.

Source Matrix Traffic

When you select the Source Matrix Traffic category, the Source Matrix Traffic window displays the traffic statistics information for each ATM RMON group, sorted by source address.

Destination Matrix Traffic

When you select the Destination Matrix Traffic category, the Destination Matrix Traffic window displays the traffic statistics information for each ATM RMON group, sorted by destination address.

ATM Accounting

The ATM accounting feature provides accounting and billing services for virtual circuits (VCs) used on the LightStream 1010 ATM switch. You enable ATM accounting on an edge switch to monitor call setup and traffic activity. A specific interface can be configured to monitor incoming,outgoing, or incoming and outgoing VC use.

Edge switches, connected to the exterior internet, are connections requiring monitoring for accounting and billing purposes.

Switching speeds and number of VCs supported by the LightStream 1010 ATM switch while monitoring VC use for can cause the amount of collected data to reach the megabyte range. With such a large amount of data in the ATM accounting files, using traditional

SNMP methods of data retrieval is not feasible. You can store the collected information in a file that you can retrieve via a file transfer protocol. SNMP messages control the selection and collection of accounting data.

A file used for data collection corresponds to two memory buffers on the ATM Switch Processor (ASP). One buffer is actively saving data; the second is passive and ready to have its data either retrieved using Trivial File Transport Protocol (TFTP) or overwritten when the currently active file reaches its maximum capacity. Using TFTP to download the file is the same as the process used to download Cisco IOS images and configuration files from the switch Flash memory to a host.

The ATM Accounting category allows you to access ATM accounting functions. When the ATM Accounting category is selected, the Data Collection Group window is displayed.

The following subcategories are available:

- Data Collection Filter
- Data Collection File
- Configuring a Data Collection File
- Enable/Disable ATM Accounting
- Enable/Disable ATM Accounting Trap
- Enable/Disable Data Collection on Interface
- Other ATM Accounting Commands

Configuring Global ATM Accounting

The ATM accounting feature must be enabled before you can gather ATM accounting VC call setup and use data. The ATM accounting feature runs in the background and captures configured accounting data for VC changes such as calling party, called party, or start time and connection type information for specific interfaces to a file.

Note Enabling ATM accounting could slow the basic operation of the LightStream 1010 ATM switch.

Timesaver To enable or disable the ATM accounting feature for the entire switch, use the **atm accounting** command. Even when ATM accounting is disabled globally, other ATM accounting commands, both global and for individual interfaces, remain in the configuration file.

Data Collection Filter

If you select the ATM Accounting category, the Data Collection Filter window opens. The Data Collection Filter window allows you to define the accounting data to be collected. Use the Select Collection Data and Select Connection Type buttons to define data collection filtering information.

Hints for Selecting Collection Data

To define the data fields, select a row in the data Collection Filter window, then consider the following:

- Collection data is listed by MIB value in the Select Connection Data window. For definitions of the MIB values, refer to the online help.
- Click **Select All** to select all listed values.
- Click **Deselect All** to deselect all values.

Hints for Selecting Connection Type

The ATM accounting selection table determines the connection data to be gathered from the switch. To select connection type(s), select a row in the ATM Accounting table, then click the Select Connection Type button.

Note A default selection is automatically configured during initial startup and cannot be deleted.

Even when ATM accounting is disabled globally, other ATM accounting commands, both global and for individual interfaces, remain in the configuration file. Features of the ATM Accounting configuration follow:

- An entry in the selection table points to a data collection file.
- A selection entry cannot be deleted when data collection is active.
- A selection entry can point to a nonexistent file, in which case the entry is considered inactive.
- One selection entry can apply to more than one type of VC (for example, SVC, PVC).
- If the next time the data collection cycle begins, it uses the new value (for example, the next time the ATM accounting collection file swap occurs).

Note The following ATM accounting MIB objects are **not** supported:
— atmAcctngTransmittedClp0Cells (object number 16)
— atmAcctngReceivedClp0Cells (object number 18)
— atmAcctngCallingPartySubAddress (object number 31)
— atmAcctngCalledPartySubAddress (object number 32)
— atmAcctngRecordCrc16 (object number 33)

Configuring a Data Collection File

The ATM accounting data being gathered from the configured selection control table should be directed to a specific ATM accounting file.

Note Only one ATM accounting file can be configured and that file cannot be deleted.

When you select the Configuring a Data Collection File category, the Data File window opens. The Data File window allows you to display or modify the accounting data file parameters. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Enable/Disable ATM Accounting

If you select the Enabling/Disabling ATM Accounting category, the Enable/Disable ATM Accounting window opens. This window allows you to enable or disable the ATM Accounting feature. To modify the configuration, select an Admin Status and click **Modify**.

Enable/Disable ATM Accounting Trap

If you select the Enable/Disable ATM Accounting Trap category, the Enable/Disable ATM Accounting Trap window opens. This window allows you to define whether accounting traps are generated on the device and what percentage of the data file size will generate the trap. To modify the configuration, select true or false to enable or disable, enter a trap threshold value, then click **Modify**. If an invalid value is entered, an error message is displayed.

Enable/Disable Data Collection on an Interface

After you enable ATM accounting, specific ingress or egress interfaces, usually on edge switches connected to the external network, must be configured to start gathering the ATM accounting data.

Modify the Enable/Disable Data Collection on an Interface table by selecting a row and right-clicking to choose true or false from the popup menu. To enable ATM accounting on a specific interface, use the following CLI commands:

Step	Command	Task
1	**configure** [**terminal**]	At the privileged EXEC prompt, enter configuration mode from the terminal.
2	**interface atm** *card/subcard/port*	Select the interface to be configured.

Step	Command	Task
3	**atm accounting**	Enable ATM accounting on the selected interface.

Other ATM Accounting Commands

When you select the Other ATM Accounting Commands category, the Other ATM Accounting Commands window opens. This window allows you to define the state of the ports that have data collection. Select states **idle** or a **cmdInProgress** (command is in progress). Set this value to **collectNow** to begin data collection, or set it to **swapToNewFile** to close the current data file and begin collection in a new file.

ATM Signaling (Global)

Signaling diagnostics enable you to diagnose a specific call failure in your network and pinpoint the location of the call failure along with the reason for the failure. To do this, you must configure a signaling diagnostics table that stores the filtering criteria and a filter index. This index is an integer between 1 and 50, used for uniquely identifying each set of filtering criteria you select. Each filtering criterion occupies one entry in the signaling diagnostics table. Each entry in the filter table is entered using the CLI commands or SNMP. Then the diagnostics software module, when enabled, filters rejected calls based on the entries in your filter table. A successful match in the filter table causes the rejected call information to be stored for analysis.

The ATM Signaling (Global) category consists of two subcategories:

- Closed User Group
- Closed User Group on Interface

When the ATM Signaling (Global) category is selected, the Configuring Closed User Group Signaling window is displayed.

Note Signaling diagnostics is a tool for troubleshooting failed calls and should not be enabled during normal switch operation.

The display table contains the records that were collected based on every filtering criteria in the filter table. Each filtering criterion has only a specified number of records stored in the table. After that number of records is exceeded, the table is overwritten.

Configuring Closed User Group Signaling

You can configure a closed user group (CUG) to form restricted access groups (virtual private networks). Different CUGs can be defined and a user can be a member of one or more CUGs. Members of a CUG can communicate among themselves, but not with users outside the group. Specific users can have additional restrictions that prevent them from originating or receiving calls from other members of the CUG. You can also specify additional restrictions on originating and receiving calls to or from members of other CUGs.

For example, if you configure three CUGs (A, B and C) in your network, you can configure them so that groups B and C can communicate with group A without restriction, but groups B and C cannot communicate with each other.You can also configure specific members of the same group to not accept calls from members of the same group.

The basis for CUGs are interlock codes. Interlock codes are unique in the whole network. Members of a CUG are assigned a unique interlock code that they use while communicating with other members of the same or different CUGs.

Interlock code is passed in CUG interlock code information element (CUG IC IE). The CUG IE also carries information that specifies whether the call can go through if the called party is not a member of the specified CUG. At the network boundary where the call originates, when a call is received from the user, the switch generates the CUG IE and sends it as part of the SETUP message. In this software release, the CUG IE only can contain the preferential CUG's interlock code. The CUG IE is used at the destination network interface to determine whether the call should be forwarded or rejected. The CUG IE is forwarded transparently by the intermediate switches.

Note End systems do not have any knowledge of interlock codes.

Two types of interlock codes are defined:

- Global interlock code is 24 bytes long and consists of a globally unique ATM End System Address (AESA) used to identify the network administering the CUG, followed by a 4-byte suffix assigned to this CUG by the network administration.
- International interlock code is 4 bytes long and consists of 4 binary coded decimal (BCD) digits containing a country code and network code, followed by a 2-byte suffix assigned to this CUG by the network administration.

Note Cisco supports only the 24-byte interlock code.

When you select the ATM Signaling (Global) category, the Configuring Closed User Group Signaling window opens. This window allows you to create a new closed user group or modify an existing group.

The action buttons are as follows:

- Create—To create a new entry, click **Create** and assign values to the fields. Then, click **Apply** to commit the configuration to the switch.
- Modify—To modify the current configuration, edit the field(s) and click **Modify** to commit the modification. If an invalid value is entered, an error message opens.

Configuring Aliases for CUG Interlock Code

You can define an alias for each CUG interlock code used on the switch. Using an alias can simplify configuration of a CUG on multiple interfaces. When you use an alias, you no longer need to specify the 48-hexadecimal-digit CUG interlock code on each interface attached to a CUG member.

To configure an alias for a CUG interlock code, use the following CLI commands:

Step	Command	Task
1	**configure** [**terminal**]	At the privileged EXEC prompt, enter configuration mode from the terminal.

Step	Command	Task
2	**atm signalling cug alias** *alias_name* **interlock-code** *interlock_code*	Configure the alias for the CUG interlock code.

Configuring CUG on an Interface

Click Create in the Closed User Group on Interface window to configure a CUG on an interface. Your first step in CUG configuration is to identify the *access interfaces.* Transmission and reception of CUG interlock codes are not allowed over access interfaces. By configuring all interfaces leading outside of the network as access interfaces, you ensure that all CUG interlock codes are generated and used only within this network.

You implement CUG procedures only if you configure the interface as an access interface.

Each access interface can be configured to permit or deny calls either *from* users attached to this interface or *to* unknown users that are not members of this interface's CUGs. In International Telecommunications Union Telecommunications Standardization Sector (ITU-T) terminology, this is called *outgoing access*. Similarly, each access interface can be configured to permit or deny calls either *to* the user(s) attached to this interface or *from* unknown users that are not members of this interface's CUG(s). In ITU-T terminology, this is called *incoming access.*

Note Interfaces to other networks should be configured as CUG access interfaces, even if no CUGs are configured on the interface. In this case, if you want the switch to exchange SVCs with the neighbor network, calls *to* and *from* unknown users should be permitted on the interface.

You can configure each access interface to have one or more CUGs associated with it, but only one CUG can be selected as the *preferential* CUG. In this software release, calls received *from* users attached to this interface can be associated only with the preferential CUG. Calls destined *to* users attached to this interface can be accepted based on membership in any of the CUGs configured for the interface.

Note You can configure CUG service without any preferential CUG. If a preferential CUG is not configured on the interface, and calls *from* users attached to this interface *to* unknown users are permitted, the calls will proceed as non-CUG calls, without generating any CUG IE.

For each CUG configured on the interface, you can specify that calls *to* or *from* other members of the same CUG be denied. In ITU-T terminology, this is called *outgoing-calls-barred* (OCB) and *incoming-calls-barred* (ICB), respectively.

Table H-1 describes the relationship between the ITU-T CUG terminology and Cisco CUG terminology:

Table H-1 Cisco CUG and ITU-T CUG Terminology Conversion

ITU-T CUG Terminology	Cisco CUG Terminology
preferential CUG	preferential
incoming access allowed	permit-unknown-cugs to-user
outgoing access allowed	permit-unknown-cugs from-user
incoming calls barred (ICB)	deny-same-cug to-user
outgoing calls barred (OCB)	deny-same-cug from-user

Enabling/Disabling a Closed User Group on Interface

If you select the Closed User Group on Interface category, the Closed User Group on Interface window opens. This window allows you to create a new entry. To create a new entry, click **Create**, and assign values to the fields. Then, click **Apply** to commit to set configuration to the switch. Select a row in the Enable CUG Service column and choose true or false from the popup menu to enable or disable the closed user group on the interface, then click **Modify**.

ATM Signaling Diagnosis

The ATM Signaling Diagnosis category consists of the following subcategories:

- Signaling Diagnosis Filter
- Enabling/Disabling Signaling Diagnosis

When the ATM Signaling Diagnosis category is selected, the Signaling Diagnosis Filter window is displayed.

Signaling Diagnosis Filter

If you select the ATM Signaling Diagnosis category, the Signaling Diagnosis Filter window opens. The Signaling Diagnosis Filter window opens and allows you to create a new entry or modify the Connection Kind, the Cast Type, the Service Category, or the Cause of Failure. You can also choose to show any Signaling Failure Records.

To create a new entry, click **Create** and assign values to the fields. After values are entered, click **Apply** to commit to set configuration to the switch. (See "Hints for Creating a Signaling Diagnosis Filter Entry" for more information.)

Hints for Creating a Signaling Diagnosis Filter Entry

When defining the fields, consider the following:

- If 0 is entered as the InifIndex value, all incoming interfaces are acted upon by this filter.
- If 0 is entered as the OutifIndex value, all outgoing interfaces are acted upon by this filter.
- If the Calling Party value is left blank, all cells are filtered, regardless of Calling Party address.
- If Called Party value is left blank, all cells are filtered, regardless of Calling Party address.
- A Max Records value of -1 means there is no limit on the number of entries.
- An Age Timeout value of -1 means this filter will not time out.

Enable/Disable Signaling Diagnosis

If you select the Enabling/Disabling Signaling Diagnosis category, the Enable/Disable Signaling Diagnosis window allows you to enable or disable the call failure filter. After selecting enable or disable, click **Modify**.

PNNI (Global)

This section describes the ATM routing and Private Network-Network Interface (PNNI) protocol implementation of the LightStream 1010 ATM switch. To place calls between ATM end systems, signaling consults an ATM routing protocol. The LightStream 1010 ATM switch provides the following ATM routing protocols:

- PNNI—A dynamic routing protocol that provides quality of service (QoS) routes to signaling based on the QoS requirements specified in the call setup request
- Interim Inter-switch Signaling Protocol (IISP)—A static routing protocol

Dynamic Routing

PNNI is a dynamic routing protocol for ATM. PNNI is dynamic because it learns the network topology and reachability information with minimal configuration. It automatically adapts to network changes by advertising topology state information.

Note In contrast, IISP is a static routing protocol. You must manually configure each route through the network. Because IISP static routing requires significant manual configuration and does not offer the scalability of PNNI hierarchy, it is best suited for use in small networks.

Source Routing

In a PNNI routing domain, the source ATM switch computes hierarchically complete routes for connection setups. This route information is included in the call setup signaling message.

In contrast, IISP uses hop-by-hop routing, where each switch that receives the connection setup message selects the next outgoing interface to which to forward the setup message. This selection is based on the mapping of destination addresses (in a routing table) to outgoing interfaces.

QoS Support

PNNI provides routes that satisfy QoS connection requests. PNNI selects routes through the network based on the administrative weight (AW) and other QoS parameters, such as the available cell rate (AvCR), maximum cell transfer delay (maxCTD), peak-to-peak cell delay variation (CDV), and cell loss ratio (CLR). The primary metric used by PNNI is AW. If a connection requests either maxCTD or CDV or both, PNNI might not be able to compute an optimum route through the network. However, PNNI guarantees a route that meets or exceeds the criteria of all specified QoS parameters.

In contrast, IISP does not provide QoS support.

PNNI Hierarchy

The primary goal of PNNI hierarchy is scalability. However, you can also use the PNNI hierarchy for other needs, such as creating an administrative boundary. For example, you can use the PNNI hierarchy to hide the internal details of one peer group from switches outside of the peer group.

The key components of PNNI hierarchy follow:

- Lowest-level nodes—A logical node in the lowest level of PNNI hierarchy.
- Peer group—A group of logical nodes. Each node exchanges information with other members of the group, and all members maintain an identical view of the group.
- Peer group leader (PGL)—A logical node within a peer group that summarizes the peer group and represents it as a single logical node at the next level of PNNI hierarchy.
- Logical group node (LGN)—A logical node that represents its lower level peer group in the next higher level peer group. Upon becoming a PGL, the PGL creates a parent LGN to represent the peer group as a single logical node at the next level. The PGL is a logical node within the peer group, and the associated LGN is a logical node in the next higher level peer group.

The lowest level of PNNI hierarchy contains lowest-level nodes only. No higher levels are possible if all nodes within a peer group are configured as lowest level nodes. If your network is relatively small and scalability is not a problem, and PNNI hierarchy is not required for other reasons, the benefits of a flat PNNI network may far outweigh the benefits of a hierarchical PNNI network. Refer to the section "Configure the Lowest Level of the PNNI Hierarchy" later in this chapter for more information.

The peer group, PGL, and LGN define the hierarchy and are needed to create multiple levels of the PNNI hierarchy. Refer to the section "Configure Higher Levels of the PNNI Hierarchy" later in this appendix for more information.

The PNNI (Global) category in CiscoView allows you to access the Private Network-Network Interface (PNNI). The following subcategories are available:

- Configure PNNI Without Hierarchy
- Configure the Lowest Level of the PNNI Hierarchy
- Configure an ATM Adress and PNNI Node Level
- Display PNNI Node Configuration
- PNNI Information
- PNNI Background Routing
- PNNI Node Config
- PNNI Node Status
- PNNI Node Config (More)
- PNNI Routing Timer
- PNNI Routing Threshold
- Enable/Disable PNNI AutoScope Mapping
- PNNI Scope Mapping-Network
- PNNI Scope Mapping-Network
- PNNI Scope Mapping-Site
- PNNI Scope Mapping-Organization
- PNNI Scope Mapping-Community

- PNNI Scope Mapping-Regional
- Enable/Disable PNNI Auto Summary
- PNNI Reachable Address Precedence
- PNNI Summary Address
- PNNI Route Address
- PNNI Route Address Status
- PNNI Route E164 Address
- Static Route Address
- PNNI Link Information
- PNNI Link Information (More)
- PNNI Neighbor Peer Statistics
- PNNI Neighbor Peer Statistics (More)
- PNNI Neighbor Peer Port
- PNNI Peer Group Leader (PGL) Election

When the PNNI (Global) category is selected, the PNNI Information window is displayed.

Configure PNNI Without Hierarchy

The LightStream 1010 ATM switch defaults to a a working PNNI configuration suitable for operation in isolated flat topology ATM networks. The switch comes with a globally unique preconfigured ATM address. Manual configuration is not required if you:

- Have a flat network topology
- Do not plan to connect the switch to a service provider network
- Do not plan to migrate to PNNI hierarchy in the future

If you plan to migrate your flat network topology to a PNNI hierarchical topology, proceed to the next section “Configure the Lowest Level of the PNNI Hierarchy.”

Configure the Lowest Level of the PNNI Hierarchy

This section describes how to configure the lowest level of the PNNI hierarchy. The lowest-level nodes comprise the lowest level of the PNNI hierarchy. When only the lowest-level nodes are configured, there is no hierarchical structure. If your network is relatively small and you want the benefits of PNNI, but do not need the benefits of a hierarchical structure, follow the procedures in this section to configure the lowest level of the PNNI hierarchy.

To implement multiple levels of PNNI hierarchy, first complete the procedures in this section and then proceed to the section "Configure Higher Levels of the PNNI Hierarchy" later in this appendix.

The lowest level PNNI configuration includes the following general procedures:

- Configuring an ATM Address and PNNI Node Level
- Configuring Static Routes
- Configuring a Summary Address
- Configuring Scope Mapping

Configuring an ATM Address and PNNI Node Level

If you are planning to implement only a flat topology network (and have no plans to migrate to PNNI hierarchy), you can skip this section and use the preconfigured ATM address assigned by Cisco Systems.

If you are planning to implement PNNI hierarchy, follow the procedure in this section to configure an ATM address and the PNNI node level.

The LightStream 1010 ATM switch is preconfigured as a single lowest-level PNNI node (locally identified as node 1) with a level of 56. The node ID and peer group ID are based on the current active ATM address.

To configure a node in a higher level of the PNNI hierarchy, the value of the node level must be a smaller number. For example, a three-level hierarchical network could progress from level 72, to level 64, to level 56. Notice that the level numbers graduate from largest at the lowest level (72) to smallest at the highest level (56).

To change the active ATM address, create a new address, verify that it exists, and then delete the current active address. After you have entered the new ATM address, disabled node 1 and then reenable it. At the same time, you can change the node level if required for your configuration. The identifiers for all higher level nodes are recalculated based on the new ATM address.

Note Node IDs and peer group IDs are not recalculated until the node is disabled and then reenabled.

Example

The following example changes the ATM address of the switch from the autoconfigured address 47.0091.8100.0000.0041.0b0a.1081.0041.0b0a.1081.00 to the new address prefix 47.0091.8100.5670.0000.0000.1122.0041.0b0a.1081.00 and causes the node identifier and peer group identifier to be recalculated:

```
Switch(config)# atm address 47.0091.8100.5670.0000.0000.1122...
Switch(config)# no atm address 47.0091.8100.0000.0041.0b0a.1081...
Switch(config)# atm router pnni
Switch(config-atm-router)# node 1 disable
Switch(config-pnni-node)# node 1 enable
Switch(config-pnni-node)#
```

Display PNNI Node Configuration

To display the ATM PNNI node configuration, use the following CLI command in user EXEC mode:

```
Switch# show atm pnni node

PNNI node 1 is enabled and running
  Node name: eng_1
  System address          47.0091810000000002EB1FFE00.0002EB1FFE00.01
  Node ID          56:160:47.0091810000000002EB1FFE00.0002EB1FFE00.00
  Peer group ID        56:160:47.0000.0000.0000.0000.0000
  Level 56, Priority 0 0, No. of interfaces 1, No. of neighbors 0
  Parent Node Index: 2
  Node Allows Transit Calls
  Node Representation: simple

  Hello interval 15 sec, inactivity factor 5,
  Hello hold-down 10 tenths of sec
  Ack-delay 10 tenths of sec, retransmit interval 5 sec,
  Resource poll interval 5 sec
  SVCC integrity times: calling 35 sec, called 50 sec,
  Horizontal Link inactivity time 120 sec,
  PTSE refresh interval 1800 sec, lifetime factor 200 percent,
  Min PTSE interval 10 tenths of sec
  Auto summarization: on, Supported PNNI versions: newest 1, oldest 1
  Default administrative weight mode: uniform
  Max admin weight percentage: -1
  Next resource poll in 3 seconds
  Max PTSEs requested per PTSE request packet: 32
  Redistributing static routes: Yes
Switch#
```

PNNI Information

When you select the PNNI (Global) category in CiscoView, the PNNI Information window displays PNNI read-only counter statistics and the supported version of the PNNI protocol for the switch device.

PNNI Background Routing

The PNNI Background Routing dialog box displays modifiable Cisco-specific PNNI background routing information and polling intervals on the device.

PNNI Node Config

The PNNI Node Config dialog box defines configuration attributes for a PNNI logical node on the device. You can change configuration parameters and create or delete a PNNI logical node.

PNNI Node Status

Use the PNNI Node Status dialog box to configure and modify the status attributes of a PNNI logical

PNNI Node config (More)

The PNNI Node Config (More) dialog box displays Cisco-specific proprietary attributes for a PNNI logical node. You can change these values for any existing node.

PNNI Routing Timer

When you select the PNNI Routing Timer category, the PNNI Routing Timer window displays timer information for the PNNI nodes defined on the device and allows you to modify the current configuration. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hints for Modifying a PNNI Routing Timer Entry

When defining the fields, consider the following:

- The PTSE Holddown value must be entered in 100s of milliseconds.
- The Hello Holddown value must be entered in 100s of milliseconds.
- The Hello Interval value must be entered in seconds. If no Hellos are triggered, this node sends a Hello packet on each of its ports at this interval.

- The PTSE Refresh Interval value must be entered in seconds.
- The PTSE Lifetime Factor value must be entered as a percentage greater than 100. Multiplying this value by the PTSE Refresh Interval produces the initial lifetime value that this node places into self-originated PTSEs.
- The Peer Delayed Ack Interval value must be entered in 100s of milliseconds.
- The AVCR Proportional Multiplier value must be entered as a percentage from 1 to 99.
- The AVCR Minimum Threshold value must be entered as a percentage from 1 to 99.
- The CDV Proportional Multiplier value must be entered as a percentage from 1 Enable/Disable o 99.
- The CTD Proportional Multiplier value must be entered as a percentage from 1 to 99.

PNNI Routing Threshold

Use the PNNI Routing Threshold dialog box to configure the significant change thresholds of QoS parameters for PNNI routing on the device.

Enable/Disable PNNI AutoScope Mapping

Use the PNNI Scope Mapping dialog box to automatically generate default PNNI scope mapping (which is not user configurable) from organizational scope values.

To change the default mapping, disable auto scope mapping by setting the row value to “manual,” which is a toggle option in each row’s popup menu, then make manual scope mapping modifications in any or all of the following PNNI Scope Mapping dialog boxes:

- PNNI Scope Mapping - Network
- PNNI Scope Mapping - Site
- PNNI Scope Mapping - Organization
- PNNI Scope Mapping - Community
- PNNI Scope Mapping - Regional

Enable/Disable PNNI Auto Summary

Use the Enable/Disable PNNI Auto Summary dialog box to enable or disable automatic generation of internal summary address(es). Automatic generation of internal summary address(es) is based on switch address(es) or node ID. Automatically generated summary addresses can only be removed by setting this object to "false."

PNNI Summary Address

Use the PNNI Summary Address dialog box to configure PNNI address summarization that may be advertised by this switch. You can change the configuration values for any defined summary address or create a new one.

Configuring a Summary Address for a PNNI Node

You can configure summary addresses to reduce the amount of information advertised by a PNNI node and contribute to scalability in large networks. Each summary address consists of a single reachable address prefix that represents a collection of end-system or node addresses. We recommend that you use summary addresses when all end-system addresses that match the summary address are directly reachable from the node. However, this is not always required because routes are always selected by nodes advertising the longest matching prefix to a destination address.

By default, each lowest-level node has a summary address equal to the 13-byte address prefix of the ATM address of the switch. This address prefix is advertised into its peer group.

You can configure multiple addresses for a single switch tobe used during ATM address migration. ILMI registers end systems with multiple prefixes during this period until an old address is removed. PNNI automatically creates 13-byte summary address prefixes from all of its ATM addresses.

You must configure summary addresses (other than defaults) on each node. Each node can have multiple summary address prefixes. Use the **summary-address** command to manually configure summary address prefixes.

Note The **no auto-summary** command removes the default summary addresses. Use the **no auto-summary** command when systems that match the first 13-bytes of the ATM addresses of your switch are attached to different switches. You can also use this command for security purposes.

Example

The following example shows how to remove the default summary address(es) and add summary address 47.009181005670:

```
Switch(config)# atm router pnni
Switch(config-atm-router)# node 1
Switch(config-pnni-node)# no auto-summary
Switch(config-pnni-node)# summary-address 47.009181005670
Switch(config-pnni-node)#
```

Displaying the Summary Address Configuration

To display the ATM PNNI summary address configuration, enter the following CLI command in user EXEC mode:

Example

The following example shows how to display the ATM PNNI summary address configuration:

```
Switch# show atm pnni summary

Codes: Node - Node index advertising this summary
       Type - Summary type (INT - internal, EXT - exterior)
       Sup  - Suppressed flag (Y - Yes, N - No)
       Auto - Auto Summary flag (Y - Yes, N - No)
       Adv  - Advertised flag (Y - Yes, N - No)

 Node Type Sup Auto Adv  Summary Prefix
 ~~~~ ~~~~ ~~~ ~~~~ ~~~
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
  1   Int   N   Y    Y   47.0091.8100.0000.0040.0b0a.2a81/104
  2   Int   N   Y    N   47.01b1.0000.0000.0000.00/80
```

Note Precedence values of 2, 3, or 4 are valid; smaller values take precedence over larger values. Local reachable addresses, whether learned through ILMI or as static routes, are given the highest priority (1).

PNNI Reachable Address Precedence

Use the PNNI Reachable Address Precedence dialog box to configure the PNNI reachable address precedence value for each address type on the device. You can change the precedence value for any reachable address type.

PNNI Route Address

Use the PNNI Route Address dialog box to display the PNNI node address that is reachable through this switch. This table is also used to configure static routes to reachable address prefixes.

Hints for Modifying a PNNI Route Address Entry

When defining the fields, consider the following:

- The Node Index field must be set to 0.
- The maximum allowable value for the Prefix Length field is 152.
- If the Local ifIndex field is set to 0, the interface is unknown.

PNNI Route Address Status

Use the PNNI Route Address Status dialog box to review the attributes of a PNNI node address that is reachable through this switch.

PNNI Route E164 Address

Use the PNNI Route E164 Address dialog box to configure and modify the proprietary attributes of the PNNI Route E164 Address.

Static Route Address

Use the Static Route Address dialog box to configure static route address information for the switch. You can change configuration information for an existing route or define a new one.

PNNI Link Information

Use the PNNI Link Information window to display link information for the PNNI nodes defined on the device.

PNNI Link Information (More)...

The PNNI Link Information (More...) dialog box lists additional attributes that describe the operation of logical links attached to the local switching system as well as the relationship of these logical links with neighbor nodes at the other end.

PNNI Neighbor Peer Statistics

When you select the PNNI Neighbor Peer Statistics category, the PNNI Neighbor Peer window displays information about the neighboring peer nodes for the PNNI nodes defined on the device in the same peer group.

PNNI Neighbor Peer Statistics (More)...

Use the PNNI Neighbor Peer Statistics (More...) dialog box to view additional attributes that describe the relationship between PNNI nodes in this switching system and neighboring nodes in the same peer group.

PNNI Neighbor Peer Port

The PNNI Neighbor Peer Ports dialog box lists read-only information about the neighboring peer node relationships for the PNNI logical nodes defined on the device in the Hello state 2-Way Inside.

PNNI Peer Group leader (PGL) Election

Use the PNNI PGL Election dialog box to configure Peer Group Leader (PGL) election information for a PNNI node on this switching system.Peer Group Election allows you to configure higher levels of the PNNI hierarchy, using the following CLI procedures:

- Configure a Logical Group Node and Peer Group Identifier
- Configure the Node Name
- Configure a Parent Node
- Configure the Node Election Leadership Priority
- Configure a Summary Address

A PNNI hierarchy configuration example follows these procedures.

After you have configured the lowest level of the PNNI hierarchy, you can complete the hierarchical structure of PNNI by configuring peer group leaders (PGLs) and logical group nodes (LGNs).

Each peer group can contain one active PGL. The PGL is a logical node within the peer group that collects data about the peer group to represent it as a single node to the next PNNI hierarchical level. Upon becoming a PGL, the PGL creates a parent LGN. The LGN represents the PGL's peer group within the next higher level peer group. The LGN aggregates and summarizes information about its child peer group and floods that information into its own peer group. The LGN also distributes information received from its peer group to the PGL of its child peer group for flooding. To create the PNNI hierarchy, select switches that are eligible to become PGLs at each level of the hierarchy. Nodes can become PGLs through the PGL election process. Each node has a configured election priority. To be eligible for election, the configured priority must be greater than zero and a parent node must be configured. Normally the node with the highest configured leadership priority in a peer group is elected PGL. You can configure multiple nodes in a peer group with a non-zero leadership priority so that if one PGL becomes unreachable, the node configured with the next highest election leadership priority becomes the new PGL.

Note The choice of PGL does not directly affect the selection of routes across a peer group.

Because any one peer group can consist of both lowest-level nodes and LGNs, lowest-level nodes should be preferred as PGLs. Configuring the network hierarchy in a manner that results in multiple LGNs at the same switch creates additional PNNI processing and slower recovery from failures. If there are switches with more processing capability (for example, because of a smaller volume of call processing compared to others), they might be more desirable for election.

We recommend that every node in a peer group that can become PGL have the same parent node configuration.

Configure a Logical Group Node and Peer Group Identifier

You can configure a new LGN by entering the **node** command with an unused node index value between 2 and 8.

The LGN is created only when the child node in the same switch (that is, the node whose **parent** configuration points to this node) is elected PGL of the child peer group.

The peer group identifier defaults to a value created from the first part of the child peer group identifier, and does not need to be specified. If you want a nondefault peer group identifier, you must configure all logical nodes within a peer group with the same peer group identifier.

Higher level nodes will only become active if:

- A lower-level node specifies the higher-level node as a parent.
- The election leadership priority of the child node is configured with a non-zero value and is elected as the PGL.

To configure a Logical Group Node, use the following commands:

Step	Command	Task
1	**configure** [**terminal**]	At the privileged EXEC prompt, enter configuration mode.
2	**atm router pnni**	Enter ATM router PNNI mode. The prompt changes to Switch(config-atm-router)#.

Step	Command	Task
3	**node** *node_index* **level** *level* [**lowest**] [**peer-group-identifier** *dd:xxx*] [**enable** | **disable**]	Configure the logical node and optionally its peer group identifier. Configure each logical node in the peer group with the same peer group identifier. When you have more than one logical node on the same switch, you must specify a different index number to distinguish it from node 1.

ILMI (Global)

The ILMI (Global) category allows you to access the Interim Local Management Interface (ILMI). The following subcategories are available:

- Switch ATM Address
- LECS Address (Global)
- Default Access Filter
- Access Filter on Interface

When the ILMI (Global) category is selected, the default window displayed is the Switch ATM Address window.

Switch ATM Address

If you select the ILMI (Global) category, the Switch ATM Address window displays the ATM address information for the switch.

The action buttons are as follows:

- Create—To create a new traffic descriptor, click **Create** and enter values in the fields. Then, click **Apply**.
- Modify—To modify the current configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message opens is displayed.

Hint for Creating/Modifying a Switch ATM Address Entry

The ATM address for this switch must be entered as 13-octet network prefixes (such as 47:00:91:81:00:0b:00:34:76:00:00:23:00) or 20-byte NSAP addresses.

LECS Address (Global)

If you select the LECS Address (Global) category, the LECS Address (Global) window displays the LECS Address table for the device. To create a new traffic descriptor, click **Create** and assign values to the fields. Then, click **Apply**.

Hint for Creating a LECS Address (Global) Entry

If the ILMI Service Registry Port value is set to 0, this row applies to all unassigned UNIs.

Default Access Filter

If you select the Default Access Filter category, the Default Access Filter window defines permission access. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Access Filter on Interface

If you select the Access Filter on Interface category, the Access Filter on Interface window opens. This window allows you to view or modify the configuration. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Managing ATM Port Features

The ATM port features allow access to the following categories:

- Resource Management (Interface)
- VCC Setup
- VPC Setup
- ATM Signaling (Interface)
- PNNI (Interface)
- ILMI (Interface)

To start the ATM port feature application, left click on an ATM port, then select **ATM Features**.

Only one category is displayed at a time. Change the category to access different management features.

To display the information for any category, select the appropriate category from the pull-down menu next to the CATEGORY label.

Note Where windows display "optional" fields, you can either enter a value or leave the field blank so the device automatically generates the value.

For additional information regarding the fields within the windows, click **Help** to access the CiscoView online help.

Resource Management (Interface)

The Resource Management (Interface) category is selected, the default window displayed is the ATM RM IF Configuration window.

The following subcategories are available:

- ATM RM IF Configuration
- ATM RM IF Service Category

- ATM RM IF sharedMem
- ATM RM IF Traffic Configuration
- ATM RM IF Traffic Configuration (More)
- ATM RM IF Statistics
- VBR Traffic Parameter
- Interface Service Category Support

ATM RM IF Configuration

If you select the Resource Management (Interface) category, the ATM RM IF Configuration window displays the Resource Management interface information for the port. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hints for Modifying the ATM RM IF Configuration Entry

When defining the fields, consider the following:

- The Pacing Rate Requested value must be entered in kilobits per second. A value of 0 disables pacing.
- The Output Pacing Rate value must be entered in kilobits per second. A value of 0 disables pacing.
- The Force Pacing value must be set to force Change if the requested pacing rate would reduce the port rate below what is currently allocated to Guaranteed Service Categories for the output flow.
- The Link Distance value must be entered in kilometers.
- Setting the Best Effort Limit value to 4294967295 disables the Best Effort limits.

ATM RM IF Service Category

If you select the ATM RM IF Service Category category, the ATM RM IF Service Category window displays the service category information for the port.

ATM RM IF sharedMem

If you select the ATM RM IF sharedMem category, the ATM RM IF sharedMem window displays the output queue information for the port. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hints for Modifying the ATM RM IF sharedMem Entry

When defining the fields, consider the following:

- The Output Queue value for the priority queues are in descending order, 91, 92, 93, and 94.
- Setting the Max Cells Requested value to 0 calculates the default automatically.
- Setting the Force Max Cells Requested Change value to forceChange allows a change in the Max Cells value; setting to noForceChange prevents such a change.

ATM RM IF Traffic Configuration

If you select the ATM RM IF Traffic Config category, the ATM RM IF Traffic Configuration window displays the traffic configuration information for specified port, and contains action buttons. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Hint for Modifying the ATM RM IF Traffic Configuration Entry

Changing the Max Aggregate Guaranteed Service value does not affect existing connections.

ATM RM IF Traffic Configuration (More)...

Use the ATM RM IF Traffic Config (More...) dialog box to configure additional traffic parameter information for this port.

ATM RM IF Statistics

If you select the ATM RM Statistics category, the ATM RM Statistics window displays the resource allocation request information for the port.

VBR Traffic Parameter

Use the VBR Traffic Parameter Config dialog box to configure traffic parameters for VBR-RT and VBR-NRT traffic types on an interface (with defaults set to 1024).

Interface Service Category Support

Use the Interface Service Category Support dialog box to configure an alternative Service Category for CBR (for the transported VCs that are allowed in the VP tunnel). Such configuration is not allowed on a non-shaped VP tunnel interface.

Note Multiple Service Categories can be configured on an interface.

VCC Setup

This section describes how to configure a typical ATM network after autoconfiguration has established the default network connections. The network configuration modifications described in this chapter are used to optimize your ATM network operation.

This section uses the following terminology:

- Virtual channel (VC)—A generic term that describes transport of ATM cells associated with a common unique identifier value.
- Virtual channel link—A means of transporting ATM cells between a point where a VCI value is assigned and the point where that value is translated or terminated.

- Virtual channel identifier (VCI)—Identifies a particular VC link for a given VPC.
- Virtual channel connection (VCC)—A concatenation of VC links that extends between two points where the adaptation layer is accessed. VCCs allow user-to-user, user-to-network, or network-to-network information transfer. Cell sequence integrity is preserved for the cells belonging to the same VCC.
- Virtual path (VP)—A generic term for a bundle of VC links: all VC links in a bundle have the same end points.
- Virtual path link—A group of VC links, identified by a common value VPI, between a point where the VPI value is assigned and the point where that value is translated or terminated.
- Virtual path identifier (VPI)—Identifies a particular VP link.
- Virtual path connection (VPC)—A concatenation of VP links that extends between two points where the VCI values are assigned and the point where those values are translated or removed. VPCs allow user-to-user, user-to-network, or network-to-network information transfer.

The characteristics of the VC, established when it is created, are:

- Quality of service (QoS)
- ATM adaption layer 5 (AAL5)
- Peak and average transmission rates
- Cell sequencing integrity

These switching features can be turned off with interface configuration commands; autonomous switching must be explicitly enabled per interface.

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

The CiscoView VCC Setup menu allows you to configure PVC parameters. When the VCC Setup menu is selected, the Cross-PVC window is displayed.

The following subcategories are available:

- Cross-PVC
- Cross-PVC Statistics
- Soft PVC
- Soft-PVC Statistics
- SVC
- SVC Statistics
- SVC Link Address
- VC Snooping

Configuring Cross-PVC

When you select the VCC Setup menu, the Cross-PVC window displays cross-PVC information and allows you to create or modify cross-PVC connections.

- Add Point-MultiPoint Leaf—To add a multipoint leaf to an existing PVC, select a point-to-multipoint PVC entry and click **Add Point-MultiPoint Leaf**. Assign values to the fields. Then click **Apply**.
- Add VC Snooping—To add VC snooping to an existing PVC, select a PVC entry and click **Add VC Snooping**. Assign values to the fields. Then, click **Apply**.

Hints for Creating/Modifying a Cross-PVC Entry

When defining the fields, consider the following:

- Cross-PVC connection creation requires the following actions:
  - Create an endpoint
  - Create a second endpoint
  - Link to the two endpoints together
  - When setting the WRR Weight value, valid weighting values are 1 to 15.

Hints for Configuring a Point-to-Point VCC

To configure a point-to-point VCC, use the following CLI commands:

Step	Command	Task
1	**configure** [**terminal**]	At the privileged EXEC prompt, enter configuration mode from the terminal.
2	**interface atm** *card/subcard/port* [*.sub-inter #*]	Select the interface to be configured.
3	**atm pvc** *vpi* [*vci* | **any-vci**[1]] [**upc** *upc*] [**pd** *pd*] [**rx-cttr** *index*] [**tx-cttr** *index*] **interface atm** *card/subcard/port*[*.vpt #*] *vpi* [*vci* | **any-vci**[2]] [**upc** *upc*]	Configure the PVC.

1 The **any-vci** parameter is only available for ATM interface 2/0/0.

Note The row index for **rx-cttr** and **tx-cttr** must be configured before this optional parameter can be used. See the section "Configure the Connection Traffic Table" in the chapter "Configuring Resource Management" of the *LightStream 1010 ATM Switch Software Configuration Guide*.

Parameter *pd* is not applicable to a virtual path.

Note When configuring PVC connections, configure the lowest VPI and VCI numbers first.

Displaying Cross-PVC Statistics

If you select the Displaying Cross-PVC Statistics category, the Cross-PVC Statistics window displays cross-PVC statistic information.

To show the VC configuration, use the following CLI commands:

Step	Command	Task
1	**show atm interface** [**atm** *card/subcard/port*]	Show the ATM interface configuration.
2	**show atm vc** [**interface atm** *card/subcard/port vpi vci*]	Show the PVC interface configuration.

Note Refer to the *LightStream 1010 ATM Switch Software Configuration Guide* for the commands needed to configure and add a point-to-multipoint leaf.

Soft-PVC

If you select the Configuring a Point-to-MultiPoint Cross PVC/PVP category, the Soft-PVC window displays soft-PVC information.

Hints for Creating/Modifying a Soft-PVC Entry

When defining the fields, consider the following:

- The SPVP Retry Interval value must be entered in seconds.
- Valid WRR Weight values are 1 to 15.

Displayling Soft-PVC Statistics

If you select the Displaying Soft-PVC Statistics category, the Soft-PVC Statistics window displays soft-PVC statistic information.

SVC

If you select the Soft-VC (SVC) category, the SVC window displays SVC information.

The action buttons are as follows:

- Create—To create a new entry, click **Create** and assign values to the fields. Then, click **Apply**.
- Modify—To modify the current configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.
- Add VC Snooping—To add VC snooping to an existing SVC, select an SVC entry and click **Add VC Snooping**. Assign values to the fields. Then click **Apply**.

Hint for Creating/Modifying an SVC Entry

Valid WRR Weight values are 1 to 15.

Displaying SVC Statistics

If you select the Displaying SVC Statistics category, the SVC Statistics window displays SVC statistic information.

SVC Link Address

If you select the SVC Link Address category, the SVC Link Address window displays the SVC link address information.

VC Snooping

If you select the VC Snooping category, the VC Snooping window displays VC snooping information.

With per-connection snooping you must specify both the snooped connection endpoint and the snooping connection endpoint. The switch IOS adds the snooping connection endpoint as a leaf to the snooped connection. The root of the temporary multicast connection depends on the direction being snooped. Snooping in the direction of leaf to root is not allowed for multicast connections. Per-connection snooping features are as follows:

- Per-VC snooping
- Per-VP snooping

The snooping connection can be configured on any port when there is no VPI/VCI collision for the snoop connection with existing connections on the port. Also, the port should have enough resources to satisfy the snoop connection resource requirements. In case of failure from a VPI/VCI collision or resource exhaustion, a warning message is displayed, and you can reconfigure the connection on a different port.

To snoop both transmit and receive directions of a connection, you need to configure two different snoop connections.

Note Per-connection snooping is available only if you have FC-FPQ installed on your ASP.

Nondisruptive per-connection snooping is achieved by dynamically adding a leaf to an existing connection (either unicast or multicast). This can lead to cell discard if the added leaf cannot process the snooped cells fast enough. For a multicast connection the queue buildup is dictated by the slowest leaf in the connection. The leaf added for snooping inherits the same traffic characteristics as the other connection leg. This ensures that the added leaf does not become the bottleneck and affect the existing connection.

To configure connection snooping, use the following CLI commands:

Step	Command	Task
1	**configure** [**terminal**]	At the privileged EXEC prompt, enter configuration mode from the terminal.
2	**interface atm** *card/subcard/port*	Specify an ATM interface and enter interface configuration mode.
3	**atm snoop-vc** [*a_vpi a_vci*] **interface atm** *card/subcard/port* x_*vpi x_vci* [**direction** {**receive** | **transmit**}]	Configure the virtual channel to be snooped. *a* denotes the snooping connection. *x* denotes the snooped connection.
4	**atm snoop-vp** [*a_vpi*] **interface atm** *card/subcard/port x_vpi* [**direction** {**receive** | **transmit**}]	Configure the virtual path to be snooped.

VPC Setup

The VPC Setup category allows you to configure PVP parameters. When the VPC Setup category is selected, the Cross-PVP window is displayed.

The following subcategories are available:

- Cross-PVP
- Cross-PVP Statistics
- Soft-PVP
- Soft-PVP Statistics
- SVP

- SVP Statistics
- SVP Link Address
- VP Snooping
- VP Tunnel

Cross-PVP

If you select the VPC Setup category, the Cross-PVP window displays cross-PVP information and allows you to create a new cross-PVP entry, modify an existing entry, or add a point-multipoint leaf or VC snooping.

The action buttons are as follows:

- Create—To create a new entry, click **Create** and assign values to the fields. Then, click **Apply**.
- Add Point-MultiPoint Leaf—To add a multipoint leaf to an existing cross-PVP, select a point-to-multipoint PVP entry and click **Add Point-MultiPoint Leaf**. Assign values to the fields. Then, click **Apply** to set configuration to the switch.
- Add VC Snooping—To add VC snooping to an existing cross-PVP, select a cross-PVP entry and click **Add VC Snooping**. Assign values to the fields. Then, click **Apply**.

Hints for Creating Cross-PVP Entry

When defining the fields, consider the following:

- Cross-PVP connection creation requires the following actions:
  - Create an endpoint.
  - Create a second endpoint.
  - Link to the two endpoints together.
- Valid WRR Weight values are 1 to 15.

Cross-PVP Statistics

If you select the Cross-PVP Statistics category, the Cross-PVP Statistics window displays cross-PVP statistic information.

Configuring Soft-PVP

If you select the Soft-PVC/PVP category, the Soft-PVP window displays soft-PVP information.

The action buttons are as follows:

- Create—To create a new entry, click **Create** and assign values to the fields, then click **Apply**.
- Add VC Snooping—To add VC snooping to an existing soft-PVP, select a soft-PVP entry and click **Add VC Snooping**. Assign values to the fields, then click **Apply**.

Soft PVC connections provide the following features:

- Connection to another host or switch that does not support signaling
- Configuration of PVCs without the manual configuration steps described in the section "Configure Permanent Virtual Channel Connections"
- Configuration of PVCs with the reroute or retry capabilities when a failure occurs in the network

Guidelines for Creating Soft PVCs

Perform the following steps when you configure soft PVCs:

Step 1 Determine which two ports you want to define as participants in the soft PVC.

Step 2 Decide which of these two ports you want to designate as the destination (or passive) side of the soft PVC.

Step 3 Configure the destination (passive) side of the soft PVC. You must configure the destination end of the soft PVC first, to define an ATM address for that port. You must retrieve this address (see Step 4), and the VPI/VCI values for the circuit (see Step 5), and use these elements as part of the command string when you configure the source (active) end of the soft PVC (see).

Step 4 Retrieve the ATM address of the destination end of the soft PVC using the **show atm address** command. This command typically produces output in the following form:

```
Switch# show atm address

Switch Address(es):
  47.00918100000000400B0A2A81.00400B0A2A81.00 active

Soft VC Address(es):
  47.0091.8100.1111.1111.1111.1111.1111.1111.1111.00 ATM4/0/0

ILMI Switch Prefix(es):
  47.0091.8100.0000.0040.0b0a.2a81

ILMI Configured Interface Prefix(es):

LECS Address(es):
Switch#
```

Step 5 Retrieve the VPI/VCI values for the circuit using the **show atm vc** [**interface atm** *card/subcard/port vpi vci*] command. This command typically produces output in the following form:

Step 6 Switch# **show atm vc interface atm 0/0/0**

Step 7 Interface VPI VCI Type X-Interface X-VPI X-VCI Encap Status

Step 8 ATM0/0/0 0 5 PVC ATM2/0/0 0 52 QSAAL DOWN

Step 9 ATM0/0/0 0 16 PVC ATM2/0/0 0 32 ILMI DOWN

Step 10 ATM0/0/0 0 200 SoftVC ATM4/0/0 0 100 UP

Step 11 Switch#

Configure the source (active) end of the soft PVC. At the same time, complete soft PVC setup using the information derived from Step 4 and Step 5.

You must configure the source end of the soft PVC last because this not only defines the configuration information for the source port but also requires that you enter the ATM address and VPI/VCI values for the destination port.

If you have not already defined the destination port for the soft PVC (as required in Step 4), this ATM address is not defined for the destination port and the VPI/VCI values are not available, as required for use in completing the soft PVC.

Configuring Soft Permanent Virtual Channel Configuration

To configure a soft PVC connection, use the following CLI commands:

Step	Command	Task
1	**show atm addresses**	Determine destination ATM address.
2	**configure** [**terminal**]	At the privileged EXEC prompt, enter configuration mode from the terminal.
3	**interface atm** *card/subcard/port* [*.vpt #*]	Select the interface to be configured.
4	**atm soft-vc** *src-vpi src-vci* **dest-address** *dest_address dest-vpi dest-vci* [**pd** *pd*] [**rx-cttr** *index*] [**slow-retry-interval** *seconds*] [**tx-cttr** *index*] [**upc** *drop pass tag*]	Configure soft PVC connection.

Note The row index for **rx-cttr** and **tx-cttr** must be configured before this optional parameter can be used. See Chapter "Configuring Resource Management" in the *LightStream 1010 ATM Switch Software Configuration Guide*.

Displaying Soft-PVP Statistics

If you select the Displaying Soft-PVP Statistics category, the Soft-PVP Statistics window displays soft-PVP statistic information.

SVP

If you select the SVP category, the SVP window displays SVP information.

SVP Statistics

If you select the SVP Statistics category, the SVP Statistics window displays SVP statistic information.

The action buttons are as follows:

- Create—To create a new entry, click **Create** and assign values to the fields, then click **Apply**.
- Add VC Snooping—To add VC snooping to an existing SVP, select an SVP entry and click **Add VC Snooping**. Assign values to the fields, then click **Apply**.

SVP Link Address

If you select the SVP Link Address category, the SVP Link Address window displays SVP link address information.

VP Snooping

If you select the VP Snooping category, the VP Snooping window displays VP snooping information.

VP Tunnel

If you select the VP Tunnel category, the VP Tunnel window displays soft-PVP information and allows you to create a new VP tunnel. To create a new tunnel, click **Create**. Assign values to the fields and click **Apply**.

ATM Signaling (Interface)

The ATM Signaling (Interface) category allows you to access the following subcategories:

- SVC Signaling Support
- ATM Signaling Statistics

When the ATM Signaling (Interface) category is selected, the default window displayed is the SVC Signaling Support window is displayed.

Configuring SVC Signaling Support

If you select the ATM Signaling (Interface) category, the SVC Signaling Support window opens. This window allows you to modify various call parameters. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Displaying ATM Signaling Statistics

If you select the Displaying ATM Signaling Statistics category, the ATM Signaling Statistics window displays ATM signaling statistics.

PNNI Interface

The PNNI Interface category displays configuration information for the PNNI interfaces defined on a port. The following subcategories are available:

- PNNI Interface
- Cisco PNNI Interface

When the PNNI Interface category is selected, the PNNI Interface window is displayed.

If you select the PNNI Interface category, the Private Network-Network Interface (PNNI) window displays configuration information for the PNNI interfaces defined on a port. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Cisco PNNI Interface

If you select the Cisco PNNI Interface category, the Cisco PNNI Interface window allows you to display or modify Cisco-specific configuration information for the PNNI interfaces defined on a port. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

ILMI Interface

The ILMI Interface category displays configuration information for the ILMI interfaces defined on a port. The following subcategories are available:

- Enable/Disable ILMI Auto Configuration
- ILMI Interface Configuration
- LECS Address (Interface)

When the PNNI Interface category is selected, the PNNI Interface window is displayed.

Enable/Disable ILMI Auto Configuration

If you select the Enabling/Disabling ILMI Auto Configuration category, the Enable/Disable ILMI Auto Configuration window opens. The window allows you to enable or disable the ILMI link and interface type determination on this device. To modify the configuration, edit the field(s) and click **Modify**. If an invalid value is entered, an error message is displayed.

Note Changes to this value take effect on the next interface restart.

ILMI Interface Configuration

If you select the ILMI Interface Configuration category, the ILMI Interface Configuration window opens. The ILMI Interface Configuration window allows you to configure the ILMI interface. To modify the current configuration, edit the field(s) and click **Modify** to commit the modification. If an invalid value is entered, an error message opens.

LECS Address (Interface)

If you select the LECS Address (Interface) category, the LECS Address (Interface) window displays the LECS address index and corresponding LECS address and allows you to create a new LECS or delete the existing LECS. To create a new LECS, click **Create** and assign values to the fields. Click **Apply**.