CHAPTER 7

Interface Configuration

You can configure or set up any interface through interface configuration windows, which are associated with each particular line card.

This chapter contains the following information:

- Generic Interface Configuration
- IP Configuration
- POS/APS Interface Configuration
- ATM Interface Configuration
- Ethernet Interface Configuration

Interfaces and Related Technology-Specific Windows

Interfaces on line cards can support multiple technologies. Configuration windows are technology-specific. For example, a POS interface supports three configurable technologies:

- Generic
- POS
- IP

Therefore, if you want to view or modify the configuration of a POS interface, you might need to view three windows:

- Generic Interface Configuration window
- POS Interface Configuration window
- IP Interface Configuration window

This same process is applicable to all different types of interfaces. The following table outlines which technology-specific configuration windows apply to each interface type.

Note Layer 3 QoS configuration, which includes CAR and WRED, is applicable for all types of interfaces. For details on CAR and WRED configuration windows, refer to Chapter 10, "Layer 3 QoS."

I

Table 7-1 Interfaces and Configuration Windows

Interfaces	Technology-Specific Configuration Windows
POS	Generic POS IP
ATM	Generic ATM IP
Ethernet	Generic Ethernet IP

Generic Interface Configuration

The Generic Interface Configuration section covers the following areas:

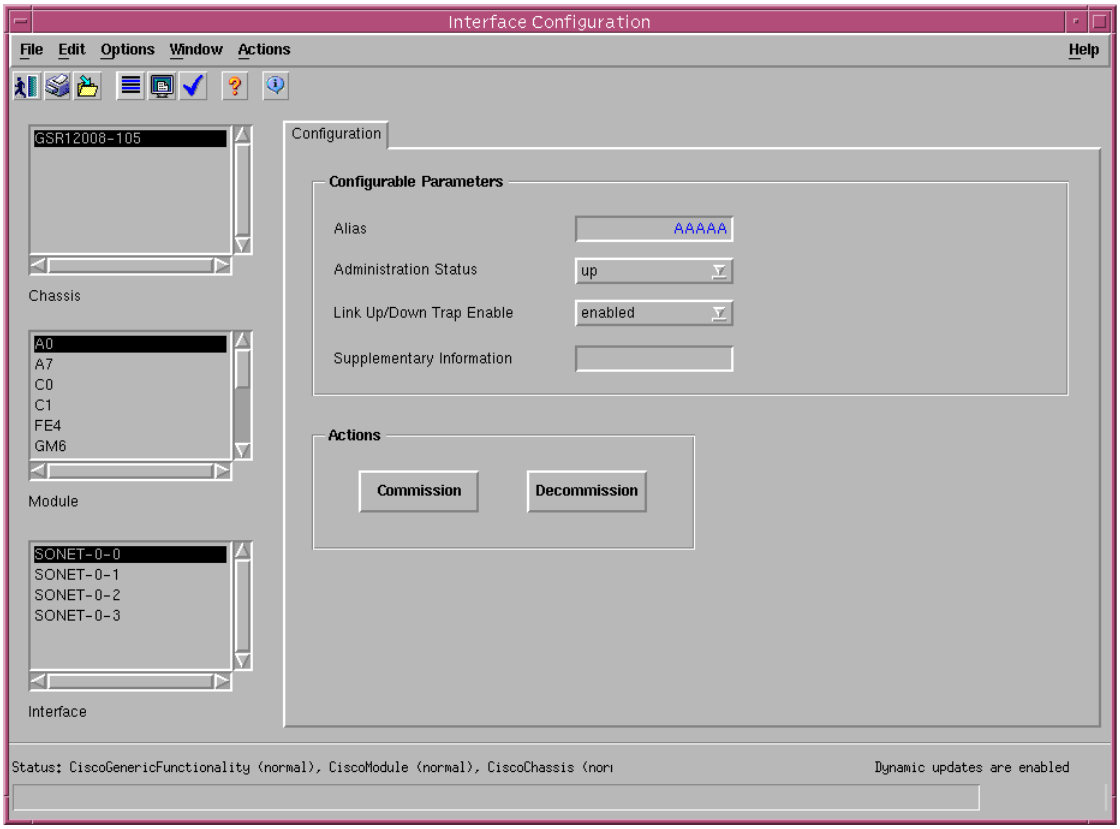
- Viewing the Generic Interface Configuration Window
- Configuring and Commissioning an Interface
- Generic Interface Configuration Window—Detailed Description

Viewing the Generic Interface Configuration Window

To view the Interface Configuration window, proceed as follows:

Right-click on any selected line card or interface, then choose **CGM Management>Physical> Interface>Generic>Configuration**. The Interface Configuration window appears.

Figure 7-1 Interface Configuration Window—Configuration Tab



Configuring and Commissioning an Interface

Tips You might want to commission an interface if you have interfaces that are not yet connected or live. For example, when you commission a chassis, subchassis discovery is automatically initiated.

Step 1 Within the Interface Configuration window, choose the chassis, module, and interface from the lists displayed at left.

Tips The status of the selected module appears at the bottom left-hand-corner of the window.

Step 2 To commission or decommission an interface:

- To commission the selected interface, click **Commission**. Commissioning the interface allows CGM to determine which state to move the interface into (typically normal).
- To decommission the selected interface, click **Decommission**. Decommissioning the interface changes its status to decommissioned.

Step 3 You can change any available information in the Configurable Parameters area. Information that is not available for selection on the particular item is grayed out.

Step 4 Click the Save icon to save the changes.

Generic Interface Configuration Window—Detailed Description

The Interface Configuration window (see Figure 7-1) contains a single Configuration tab.

Configuration Tab

The Configuration tab contains two areas: Configurable Parameters, and Actions.

Configurable Parameters

The Configurable Parameters area contains the following fields:

Alias—Name for the interface, as specified by the network manager.

Administration Status—Allows you to enable, disable or reset the module.

Link Up/Down Trap Enable—Allows you to choose whether link up/down traps should be generated for this interface.

Supplementary Information—Supplementary information.

Actions

The Actions area allows you to commission or decommission a selected interface.

Commission—Click **Commission** to commission the selected interface.

Decommission—Click **Decommission** to decommission the selected interface.

IP Configuration

The IP Configuration window allows you to configure generic IP fields (such as IP address, interface state, and so on).

The IP Configuration section covers the following areas:

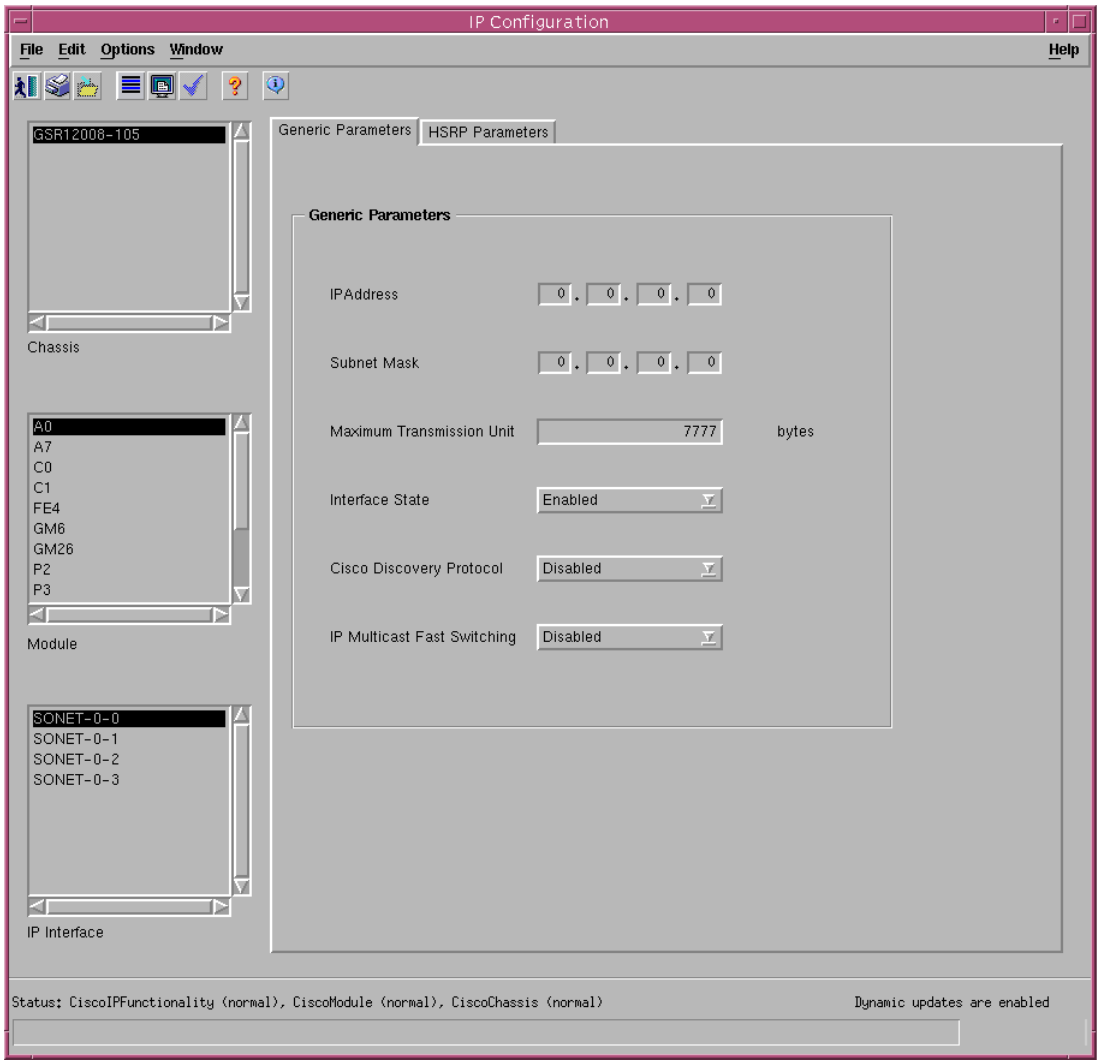
- Viewing the IP Configuration Window
- IP Configuration Window—Detailed Description

Viewing the IP Configuration Window

To view the IP Configuration window, proceed as follows:

Step 1 Right-click a selected IP line card or IP interface, then choose **CGM Management>Physical> Interface>IP>Configuration**. The IP Configuration window appears, with the Generic Parameters tab displayed.

Figure 7-2 IP Configuration Window—Generic Parameters Tab



Step 2 Choose a chassis, module, and IP interface from the lists displayed on the left hand side of the window.

Step 3 You can now configure any of the fields in the tabs. For detailed information on the fields within the tabs, refer to the section below.

Step 4 Click **Save** when you are finished.

IP Configuration Window—Detailed Description

The IP Configuration window (see Figure 7-1) contains two tabs: Generic Parameters and HSRP Parameters.

Generic Parameters Tab

The Generic Parameters tab contains a single Generic Parameters area.

Generic Parameters

The Generic Parameters area contains the following fields:

IP Address—IP address for the selected chassis.

Subnet Mask—Address mask for the selected chassis.

Maximum Transmission Unit—Maximum packet size, in bytes, that the selected interface can handle.

Interface State—Choose the interface state to be used from the drop down list.

Cisco Discovery Protocol (CDP)—Enable or disable CDP on the chassis. CDP allows a device to advertise its existence to other devices and receive information about other devices on the same LAN or on the remote side of a WAN.

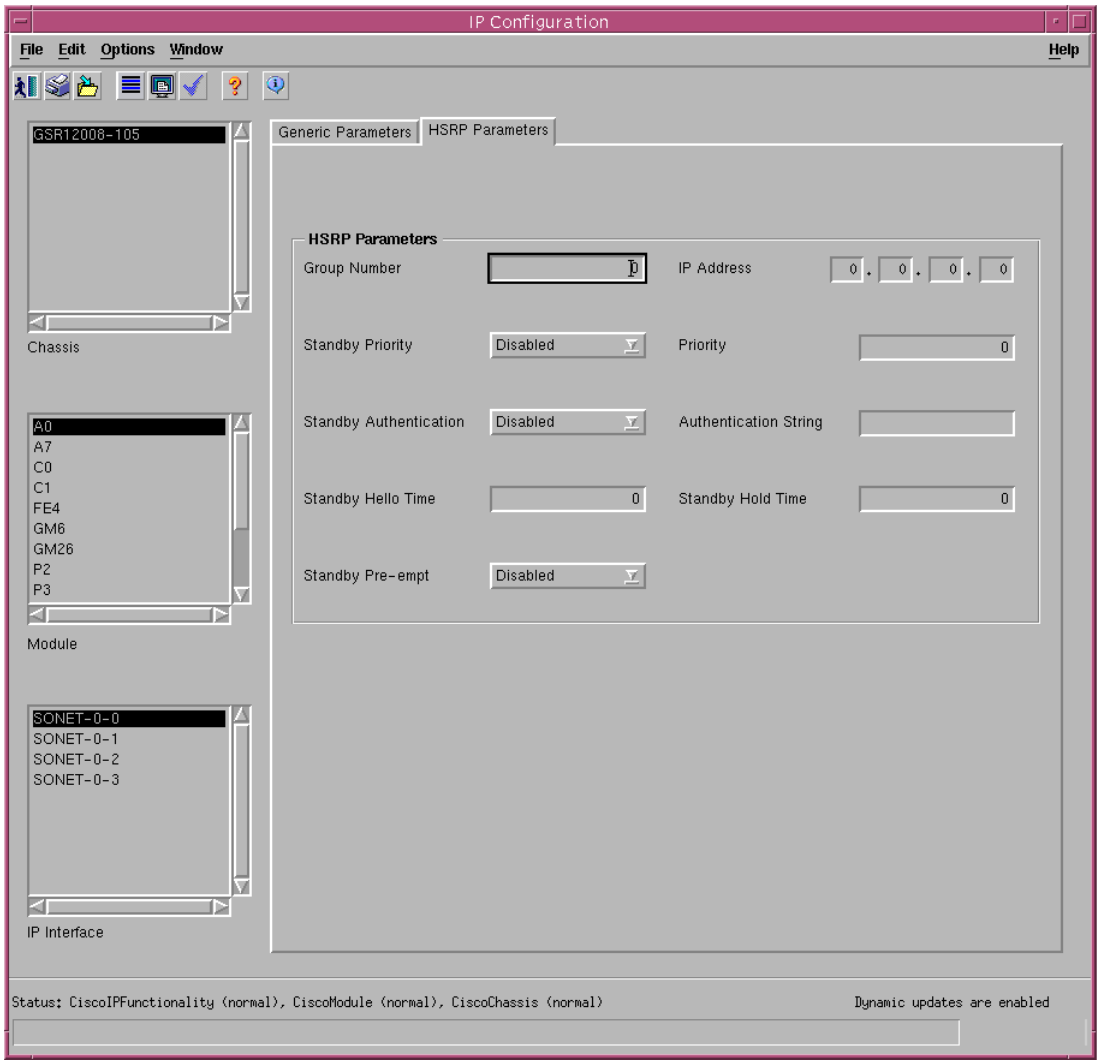
IP Multicast Fast Switching—Enable or disable IP Multicast Fast Switching on the chassis.

HSRP Parameters Tab

The HSRP Parameters tab appears as follows.

Note CGM can only support the configuration of one HSRP group.

Figure 7-3 IP Configuration Window—HSRP Parameters Tab



The HSRP Parameters tab contains a single HSRP Parameters area, and the following individual field:

HSRP Profile Name—If you have created and applied an HSRP profile to the selected interface, that profile name appears here.

HSRP Parameters

The HSRP Parameters area contains the following fields:

Group Number—Group number on the interface for which HSRP is being activated. The default is zero.

IP Address—IP address of the hot standby router interface.

Standby Priority—Enable or disable the priority for the HSRP interface. Possible values are as follows:

Enabled—When the current interface fails, it automatically switches to the standby interface.

Disabled—When the current interface fails, it does not switch to a standby interface.

Priority—Priority value that prioritizes a potential hot standby router. The range is 1 to 255; the default is 100.

Standby Authentication—Enable or disable the standby authentication string. Options available are:

Enabled—Checks for an authentication string set and allows you to configure the interface on presence of the set string.

Disabled—Does not check for an authentication string.

Authentication String—Serves as check to avoid any damage to the interface. It can be up to eight characters in length. The default string is "cisco."

Standby Hello Time—(in seconds) Can be an integer from 1 to 255. The default is 3 seconds.

Standby Hold Time—Set the time in seconds before the active or standby router is declared to be down. This is an integer from 1 to 255. The default is 10 seconds.

Standby Preempt—Standby router waits for the set time and takes over as active router if the current router fails or does not respond to the packets sent.

POS/APS Interface Configuration

POS/APS Configuration includes the following actions:

- Configure a POS interface (including General, SONET Overhead, Alarm Reporting and Threshold fields)
- Configure or remove APS (Automatic Protection Switching)

Note It is recommended that only a system administrator have access to the APS configuration window.

The POS/APS Interface Configuration section covers the following areas:

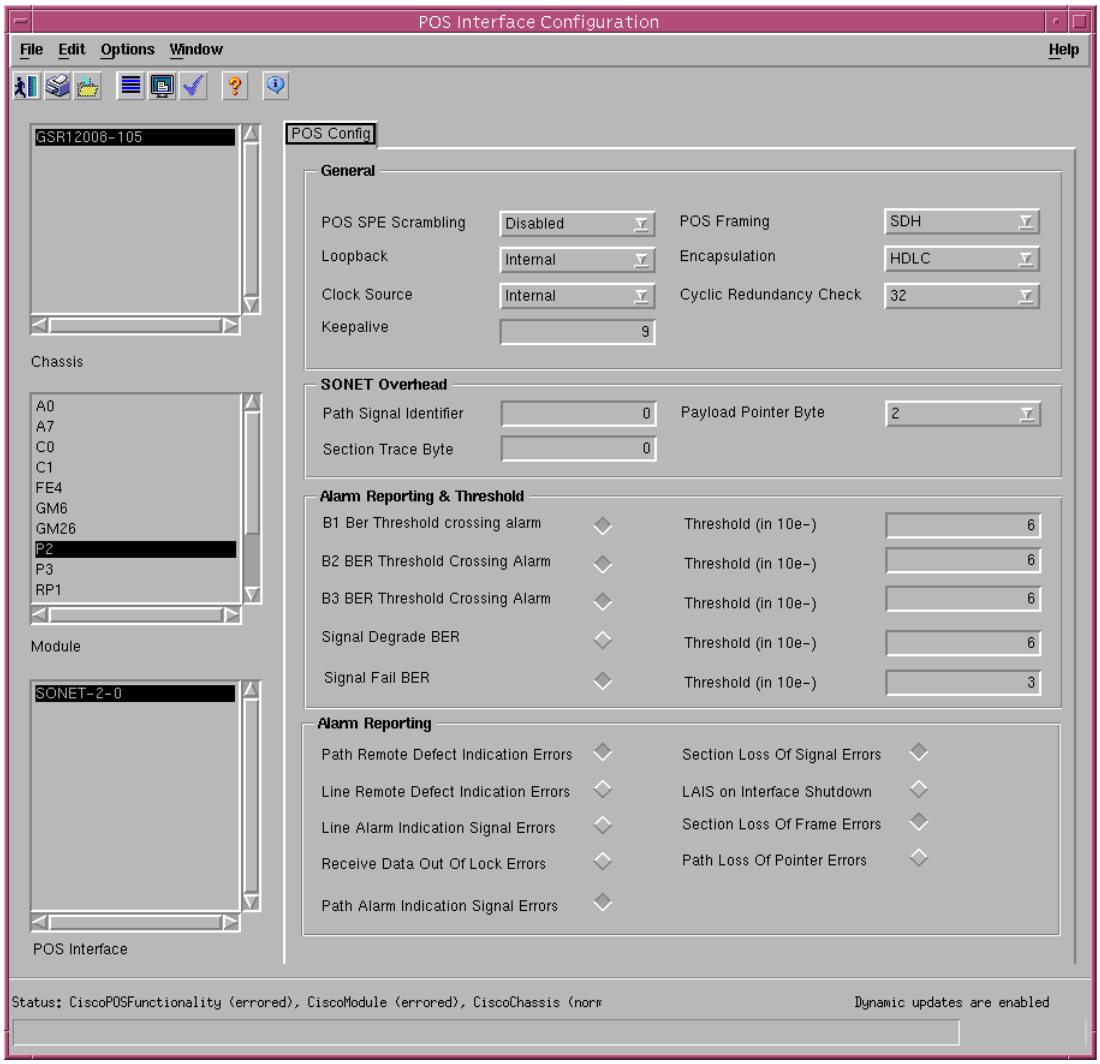
- Viewing the POS Interface Configuration Window
- POS Interface Configuration Window—Detailed Description
- Viewing the APS Configuration Window
- APS Configuration Window—Detailed Description

Viewing the POS Interface Configuration Window

To view the POS Interface Configuration window, proceed as follows:

Step 1 Right-click on a selected POS line card or POS interface, then choose **CGM Management>Physical> Interface>POS>Configuration**. The POS Interface Configuration window appears.

Figure 7-4 POS Interface Configuration Window—POS Config Tab



Step 2 Choose a chassis, module, and POS interface from the lists displayed on the left hand side of the window.

Step 3 You can now configure any of the fields in the tab. For detailed information on the fields within this tab, refer to "POS Interface Configuration Window—Detailed Description."

Step 4 Click **Save** when you are finished.

Step 5 You can proceed to the APS configuration window if desired.

POS Interface Configuration Window—Detailed Description

The POS Interface Configuration window contains one tab, POS Config.

POS Config Tab

The POS Config tab (see Figure 7-4) contains four areas: General, SONET Overhead, Alarm Reporting and Threshold, and Alarm Reporting.

General

The General area contains the following fields:

Profile Name—POS profile name applied to the selected interface.

POS SPE Scrambling—Enable or disable POS SPE scrambling. Scrambling is similar to encrypting. The enabled option is selected by default.

POS Framing—Choose the type of POS framing.

Loopback—Choose the loopback mode. The following options are available:

Enabled—Packets are transmitted back to the source to test the interface functionality and ensure that packets transmitted through the interface reach the destination without data loss.

Disabled—Restricts connection status (success or failure) messages from being received.

Encapsulation—Select HDLC, PPP or Frame-Relay encapsulation type.

Clock Source—Choose a clock source from the available options. There is a clock in every device, which measures the speed of the device. This can either be internal (within the device) or line (network clock).

Cyclic Redundancy Check—Choose an option for cyclic redundancy check. Cyclic redundancy checks consist of 16 or 32 bit encryption code which have to be same at both the transmitting and receiving ends to ensure the packets sent are received in full without loss of data. By default, it is 32 bit code.

Keepalive—Set keepalive period. The system sends packets to know if the interface or the network is up for routing packets. By default it is 10 seconds.

SONET Overhead

The Sonet Overhead area contains the following fields:

Path Signal Identifier—Permissible values range from 0 to 255; the default value is 0x16.

Payload Pointer Byte—Choose an option for payload pointer byte from the drop down menu. Permissible values range from 0 to 3.

Section Trace Byte—Permissible values are 0x1 or 0xCC; the default value is 0xCC.

Alarm Reporting & Threshold

The Alarm Reporting & Threshold area allows you to configure and enable alarms generated by the system. This area contains the following fields:

B1 BER Threshold Crossing Alarm (TCA)—Set threshold limits for the system to prompt appropriate B1 BER TCA threshold alarm messages. The field beside this value displays the threshold for the B1 BER TCA.

B2 BER Threshold Crossing Alarm (TCA)—Set threshold limits for the system to prompt appropriate B2 BER TCA threshold alarm messages. The field beside this value displays the threshold for the B2 BER TCA.

B3 BER Threshold Crossing Alarm (TCA)—Set threshold limits for the system to prompt appropriate B3 BER TCA threshold alarm messages. The field beside this value displays the threshold for the B3 BER TCA.

Signal Degrade BER—Set threshold limits for the system to prompt appropriate signal degrade ber threshold alarm messages. The field beside this value displays the threshold for the signal degrade BER.

Signal Fail BER—Set threshold limits for the system to prompt appropriate signal fail BER threshold alarm messages. The field beside this value displays the threshold for the signal fail BER.

Alarm Reporting

The Alarm Reporting area contains the following fields:

Path Remote Defect Indication Errors—Enable or disable the path remote defect indication errors alarm messages.

Section Loss of Signal Errors—Enable or disable the section loss of signal errors alarm messages.

Line Remote Defect Indication Errors—Enable or disable the line remote defect indication errors alarm messages.

LAIS on Interface Shutdown—Enable or disable the LAIS on interface shutdown alarm messages.

Line Alarm Indication Signal Errors—Enable or disable the line alarm indication signal errors alarm messages.

Section Loss of Frame Errors—Enable or disable the section loss of frame errors alarm messages.

Receive Data Out of Lock Errors—Enable or disable the Receive data output of lock errors alarm messages.

Path Loss of Pointer Errors—Enable or disable the path loss of pointer errors alarm messages.

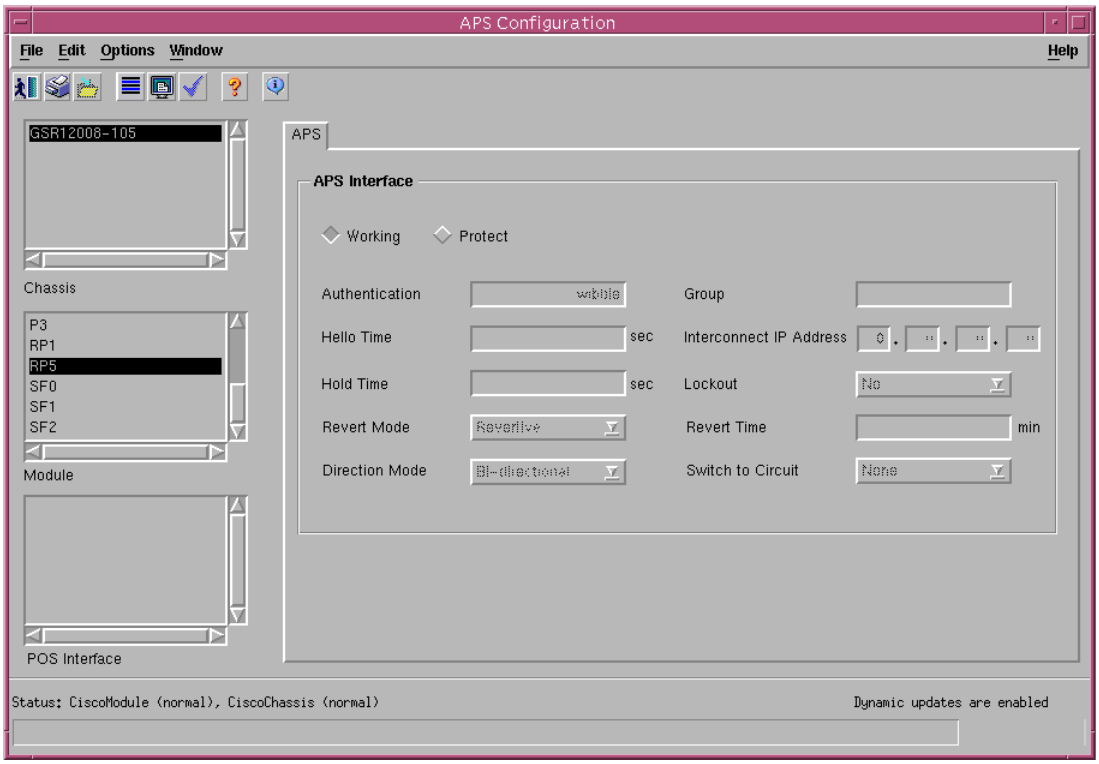
Path Alarm Indication Signal Errors—Enable or disable the path alarm indication signal errors alarm messages.

Viewing the APS Configuration Window

To view the APS Configuration window, proceed as follows:

Step 1 Right-click on a selected POS line card or POS interface, then choose **CGM Management>Physical>Interface>POS>APS Configuration**. The APS Configuration window appears.

Figure 7-5 APS Configuration Window—APS Tab



Step 2 Add or remove a working or protected interface, as desired. For details, see below.

The APS Configuration window allows you to do the following:

- Add a working interface
- Remove a working interface
- Add a protected interface
- Remove a protected interface

Adding a Working Interface

To add a working interface, proceed as follows:

Step 1 Select the relevant chassis, module, and POS interface from the list boxes at left.

Step 2 Select the **Working** button.

Step 3 Enter appropriate text in the Authentication and Group fields (for details on these fields, refer to "APS Configuration Window—Detailed Description.")

Step 4 Click **Save**.

Removing a Working Interface

To remove a working interface, proceed as follows:

Step 1 Select the relevant chassis, module, and POS interface from the list boxes at left.

Step 2 The **Working** button for the selected interface should already be selected. Click the **Working** button to deactivate.

Step 3 Click **Save**.

Adding a Protected Interface

To add a protected interface, proceed as follows:

Step 1 Select the relevant chassis, module, and POS interface from the list boxes at left.

Step 2 Select the **Protect** button.

Step 3 Enter appropriate text in all fields (for details on these fields, refer to "APS Configuration Window—Detailed Description.")

Step 4 Click **Save**.

Removing a Protected Interface

To remove a protected interface, proceed as follows:

Step 1 Select the relevant chassis, module, and POS interface from the list boxes at left.

Step 2 The **Protect** button for the selected interface should already be selected. Click the **Protect** button to deactivate.

Step 3 Click **Save**.

APS Configuration Window—Detailed Description

The APS Configuration window contains one tab, APS.

APS Tab

The APS tab (see Figure 7-5) contains one area, APS Interface.

APS Interface

The APS Interface area contains the following buttons and fields:

Working—Select this button to establish a working interface.

Protect—Select this button to establish a protected interface.

Authentication—Allows you to set values, which serve as check on entry of packets (information) sent over the network. This shields the system from any damage on account of data download.

Hello Time—Set time for the working interface to report on its status to the protected interface. The interface is bidirectional by default.

Hold Time—Set the time for protected interface (standby system) to wait for the working interface to communicate on its status. On expiry of time set, the protected interface takes over and is currently the working or the active interface.

Revert Mode—Setting the mode to "Revertive" will enable automatic switch-over from the protect interface to the working interface after the working interface becomes available.

Direction Mode—Choose the interface direction mode. Options available are:

Unidirectional—Packets are received and transmitted independently.

Bidirectional—Packets are transmitted and received in pairs.

Group—Has a value of 1 for each interface established.

Interconnect IP Address—IP Address of the router that contains the working interface.

Lockout—Set the value to yes or no. Yes prevents the working interface from switching to the protected interface.

Revert Time—Set the revert time, the system reverting automatically to the working interface from protected interface (standby system) once the working interface is online.

Switch to Circuit—Set the value for the circuit to switch to protected interface when working interface fails. The options are: manual, force, or none.

ATM Interface Configuration

The ATM Interface Configuration section covers the following areas:

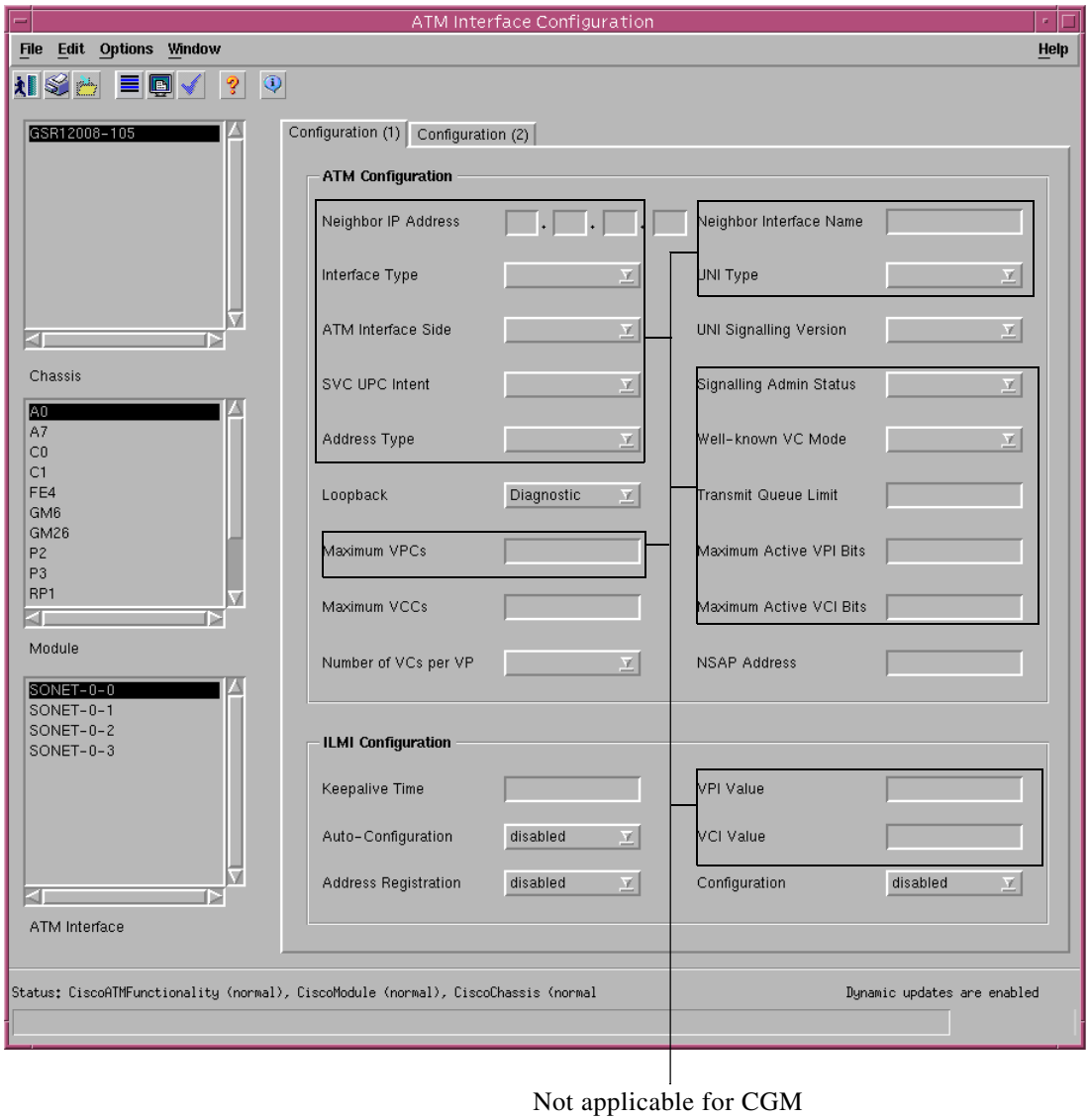
- Viewing the ATM Interface Configuration Window
- ATM Interface Configuration Window—Detailed Description

Viewing the ATM Interface Configuration Window

To view the ATM Interface Configuration window, proceed as follows these steps:

Step 1 Right-click on a selected ATM line card or ATM interface, then choose **CGM Management> Physical>Interface>ATM>Configuration**. The ATM Interface Configuration window appears.

Figure 7-6 ATM Interface Configuration Window—Configuration 1 Tab



Step 2 Choose a chassis, module, and ATM interface from the lists displayed on the left hand side of the window.

Step 3 You can now configure any of the fields in both tabs. For detailed information on the fields within these tabs, refer to the section below.

Step 4 Click **Save** when you are finished.

ATM Interface Configuration Window—Detailed Description

The ATM Interface Configuration window contains two tabs: Configuration (1) and Configuration (2).

Configuration (1) Tab

The Configuration (1) tab (see Figure 7-6) contains two areas: ATM Configuration, and ILMI Configuration.

ATM Configuration

The ATM Configuration area contains the following fields:

Neighbor IP Address—Not applicable for CGM.

Neighbor Interface Name—Not applicable for CGM.

Interface Type—Not applicable for CGM.

UNI Type—Not applicable for CGM.

ATM Interface Side—Not applicable for CGM.

UNI Signalling Version—Version of UNI signalling that is currently being used on the interface. The appropriate value, either atmfUni3Dot0, atmfUni3Dot1, or atmfUni4Dot0, is used when the interface is an UNI or IISP interface. The value not applicable is used when the interface is a PNNI interface or when signalling is disabled. Setting this variable to a value of not applicable is not allowed. To modify this field, the interface admin status has to be down and the interface Ilmi auto configuration disabled.

SVC UPC Intent—Not applicable for CGM.

Signalling Admin Status—Not applicable for CGM.

Address Type—Not applicable for CGM.

Well-known VC Mode—Not applicable for CGM.

Loopback—The following options are available:

Enabled—Packets are transmitted back to the source to test the interface functionality and ensure that packets transmitted through the interface reach the destination without data loss.

Disabled—Restricts connection status (success or failure) messages from being received.

Diagnostic—Transmit data stream is looped to the transmit direction.

Transmit Queue Limit—Not applicable for CGM.

Maximum VPCs—Not applicable for CGM.

Maximum Active VPI Bits—Not applicable for CGM.

Maximum VCCs—Maximum number of VCCs (PVCs and SVCs) supported at this interface.

Maximum Active VCI Bits—Not applicable for CGM.

Number of VCs per VP—Set the number of virtual channel per virtual path.

NSAP (Network Service Access Point) Address—Specify the NSAP address.

ILMI Configuration

The ILMI Configuration area contains the following fields:

Keepalive Time—Amount of time that should elapse between successive ILMI keepalive messages sent on this interface. A value of 0 disables ILMI keepalive messages on this interface.

VPI Value—Not applicable for CGM.

Auto-Configuration—Enable or disable the ILMI link and interface type determination. The configuration takes effect only on the next interface restart.

VCI Value—Not applicable for CGM.

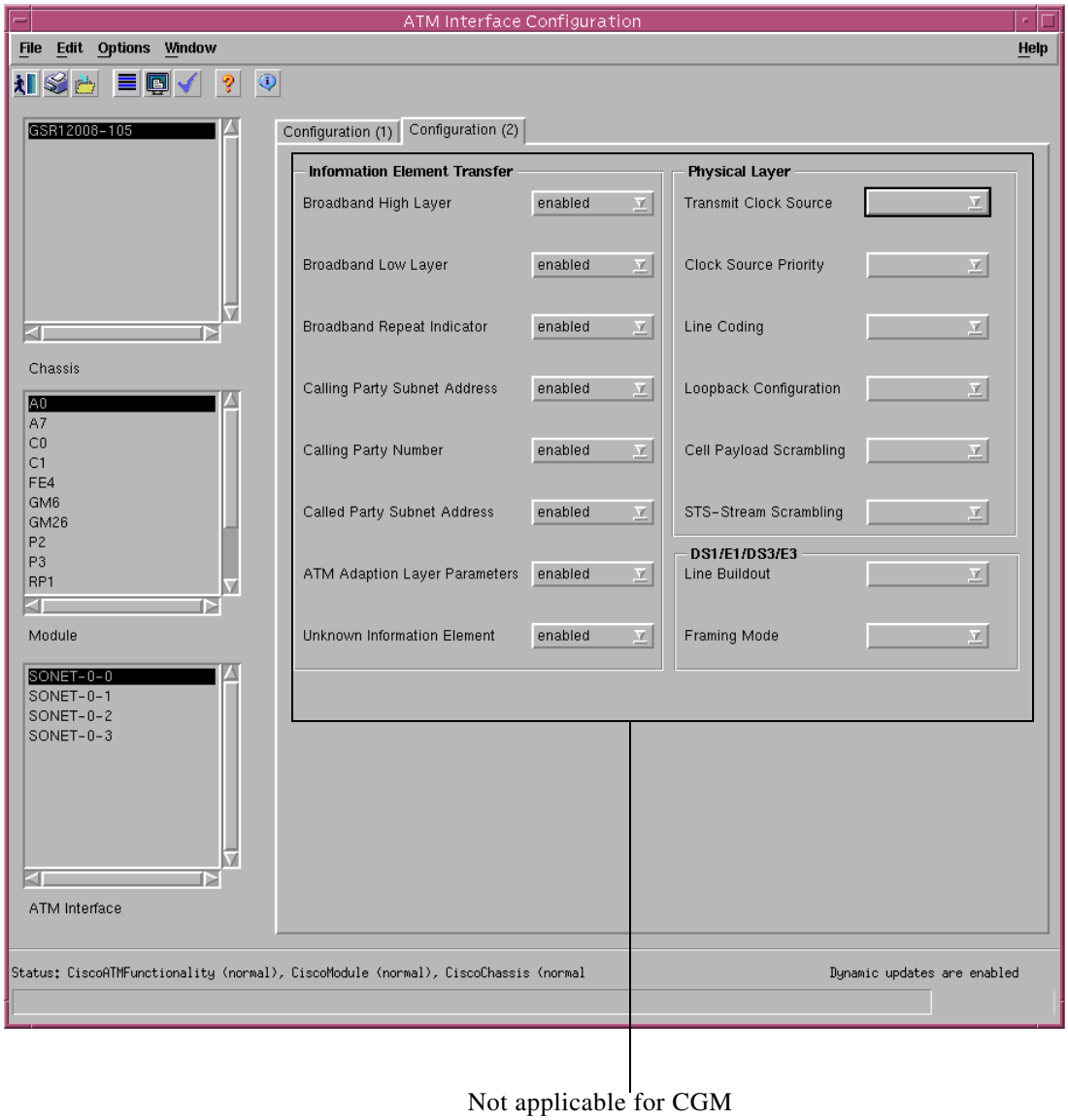
Address Registration—Enable or disable ILMI address registration on this interface. The configuration takes effect only on the next interface restart.

Configuration—Enable or disable ILMI configuration on this interface. The configuration takes effect only on the next interface restart. Disabling this object will also disable address registration, auto-configuration, and keepalive time.

Configuration 2 Tab

The Configuration (2) tab contains three areas: Information Element Transfer, Physical Layer, and DS/E1/DS3/E3. The Configuration 2 tab appears as follows.

Figure 7-7 ATM Interface Configuration—Configuration (2) Tab



Information Element Transfer

The information displayed in the Information Element Transfer area is not applicable for CGM.

Physical Layer

The information displayed in the Physical Layer area is not applicable for CGM.

DS1/E1/DS3/E3

The information displayed in the DS1/E1/DS3/E3 area is not applicable for CGM.

Ethernet Interface Configuration

The Ethernet Interface Configuration window allows you to configure Ethernet fields, such as loopback, keepalive period, and MAC address.

The Ethernet Interface Configuration section covers the following areas:

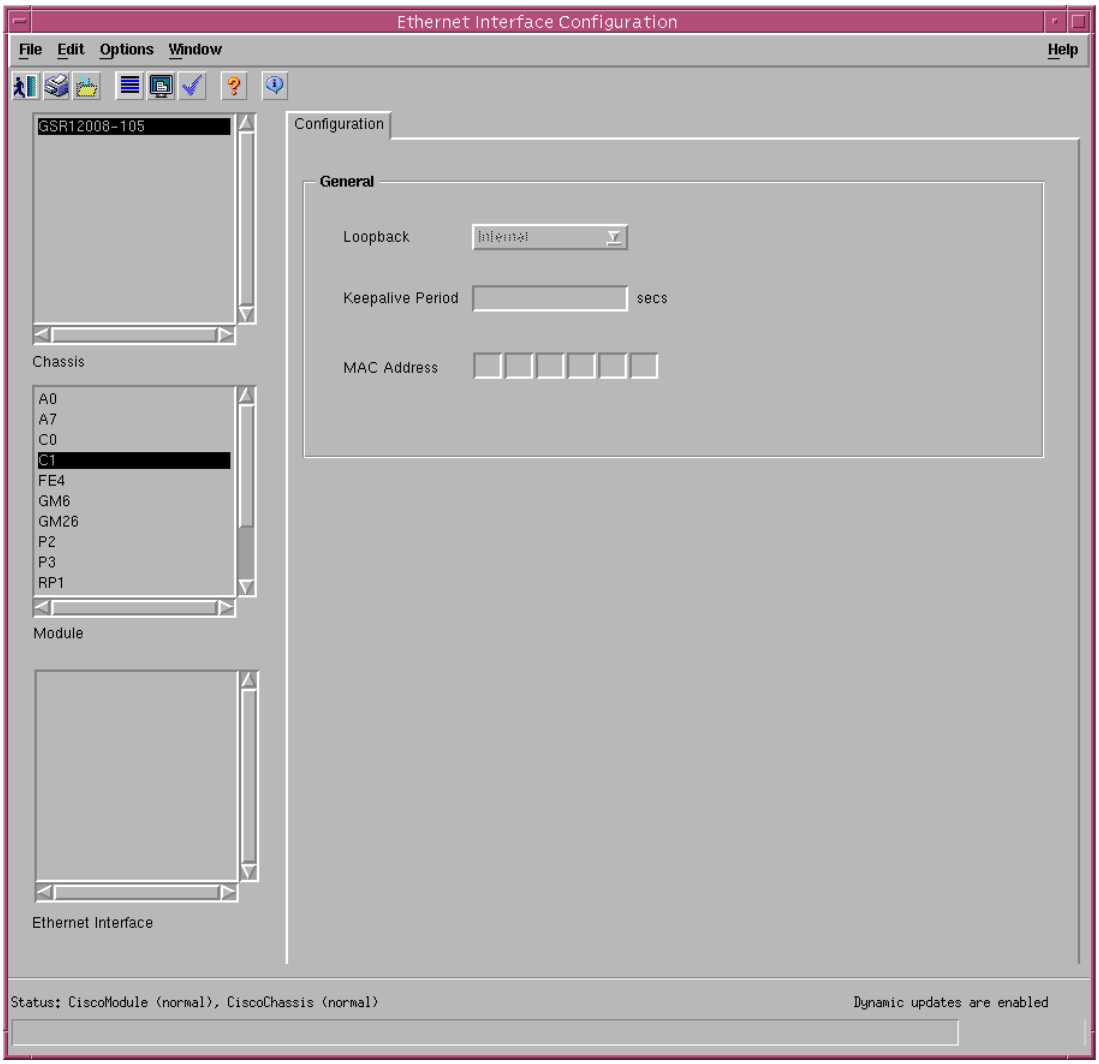
- Viewing the Ethernet Interface Configuration Window
- Ethernet Configuration Window—Detailed Description

Viewing the Ethernet Interface Configuration Window

To view the Ethernet Interface Configuration window, follow these steps:

Step 1 Right-click on a selected Ethernet line card or an Ethernet interface, then choose **CGM Management> Physical>Interface>Ethernet>Configuration**. The Ethernet Interface Configuration window appears.

Figure 7-8 Ethernet Interface Configuration Window—Configuration Tab



Step 2 Choose a chassis, module, and Ethernet interface from the lists displayed on the left hand side of the window.

Step 3 Enter the relevant values, using the drop-down lists and data entry boxes.

Step 4 Click the **Save** icon to save the changes made.

For further information on the fields displayed in this window, refer to "Ethernet Configuration Window—Detailed Description" section on page 7-19

Ethernet Configuration Window—Detailed Description

The Ethernet Interface Configuration window contains a single Configuration tab.

Configuration Tab

The Configuration tab (see Figure 7-8) contains a single General area.

General

The General area contains the following fields:

Loopback—The following options are available:

Internal—No cable is needed to connect the input and output ports. The data is looped back within the device itself. Applicable only for Gigabit and Fast Ethernet interfaces.

External—Input and output ports are physically connected by a cable to simulate a loopback. When data is transmitted, it travels through the output port and enters the device through the input port. Applicable only for Gigabit and Fast Ethernet interfaces.

Enabled—Packets are transmitted back to the source to test the interface functionality and ensure that packets transmitted through the interface reach the destination. Applicable only for GRP Ethernet interfaces.

Caution When the loopback for the Ethernet interface in the GRP is enabled, the Ethernet communication link to the GSR will be lost.

Disabled—Restricts connection status (success or failure) messages from being received. Applicable for GRP Ethernet interfaces and Gigabit and Fast Ethernet interfaces.

Keepalive Period—Displays set the keepalive period. The system sends packets to know if the interface or the network is up for routing packets. By default it is 10 seconds.

MAC Address—Specify the MAC address of the interface. Each interface is identified by a unique MAC address.