Cisco Systems

Cisco DSL Manager NI-2 User Guide

Release 3.4
March 22, 2002

Corporate Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
http://www.cisco.com
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 526-4100

Text Part Number: OL-2076-01

CONTENTS

FIGURES

TABLES

Preface

This preface explains the audience, purpose, and organization of the *Cisco DSL Manager NI-2 User Guide*. It also defines the conventions that are used to present instructions and information.

Audience

The *Cisco DSL Manager NI-2 User Guide* is designed for network managers, system administrators, and operators. This guide is also written for central office (CO) technicians and maintenance personnel who are familiar with telco products and networking systems.

This guide assumes that you have a basic understanding of network design, operation, and terminology, and that you are familiar with the configuration specifications of your own networks. This guide also assumes that you have a basic familiarity with UNIX, and that you have read the *Cisco Element Management Framework User Guide*.

Purpose

The *Cisco DSL Manager NI-2 User Guide* describes how to use the Cisco Digital Subscriber Line (DSL) Manager (CDM) graphical user interface (GUI) to manage the Cisco 6015, 6100, 6130, 6160, and 6260 DSLAM chassis that have a network interface-2 (NI-2) configuration. This guide includes descriptions of menus, dialog boxes, system files, and events and alarms. This guide also provides instructions for navigating in CDM, configuring your system, monitoring subscriber status and configuration settings, saving and restoring configuration data, and upgrading the node software. For additional information on related documentation, see the "Related Documentation" section on page xxviii.

Organization

The *Cisco DSL Manager NI-2 User Guide* is organized as follows:

- Chapter 1, "Overview of the CDM Graphical User Interface," provides a general overview for using the Cisco Digital Subscriber Line Manager (CDM) graphical user interface (GUI) to manage the Cisco DSLAM chassis and other network components. This chapter also describes how to navigate through the GUI.

- Chapter 2, "Getting Started Using CDM," describes the tasks you must perform to begin working with CDM. To manage Cisco DSLAMs on the network, you should be familiar with the Cisco EMF and CDM GUIs. This chapter briefly describes the Cisco EMF portion of the software, but mainly describes the CDM user interface.
- Chapter 3, "Creating and Applying xDSL Profiles," describes how to create, apply, and delete *x*DSL subscriber profiles.
- Chapter 4, "Creating Connections and ATM QoS Profiles," describes how to use the connection synchronization policy feature, how to create PVCs and SPVCs, how to manage virtual channels links (VCLs), how to manually upload ATM connections and create ATM quality of service (QoS) profiles, and how to use inverse multiplexing over ATM (IMA) on Cisco 6015 and 6160 DSLAMs.
- Chapter 5, "Configuring Subtend Configurations," describes how to configure subtending systems and how to set subtended subscriber PVCs. Subtending allows you to use one ATM backbone for multiple Cisco DSLAMs.
- Chapter 6, "Maintaining System Performance," describes how to maintain your Cisco EMF and CDM software system at its peak level of performance.
- Chapter 7, "Viewing System and Object Status."describes the windows in CDM that you can open to observe system and network object status.
- Chapter 8, "Viewing Performance Data," describes the interface performance windows in which you can view real-time, current performance information within 10-second polled intervals for interfaces and line cards. This chapter also describes how to access CDM windows that display historical performance data.
- Chapter 9, "Viewing Inventory and Summary Information," describes how to access inventory details about Cisco DSLAM chassis and each of the cards within the chassis. This chapter also describes the Chassis Summary Data window where you can view summary information about chassis, modules, PVCs, subscribers, and other managed objects. Additionally this chapter describes the Interface Summary window through which you can view data about specific interfaces.
- Appendix A, "Viewing Alarms and Events," describes how to identify faults (events or alarms) that a Cisco DSLAM generates on the network. When a fault occurs on a managed object in the network, CDM receives immediate notification. When you open the Cisco EMF Event Browser from the launchpad, a color next to the network object indicates the presence of an alarm.
- Appendix B, "Creating User Groups and Using the Technology-Specific Commands," includes information and instructions for creating user groups through the Cisco EMF Groups application and for using the technology-specific commands from the Tools menu.
- Appendix C, "Using the Cisco DSL Manager Object Menus," provides detailed descriptions of the object menus that you can access from the Cisco DSL Manager menu.
- Appendix D, "Finding Tasks and Related Windows," lists tasks for setting up and managing DSLAMs through the CDM GUI, identifies the associated windows, and includes links to the related procedures.
- Glossary.
- Index.

Conventions

This publication uses the document conventions listed in this section.

Table 1 Font Conventions

Convention	Definition	Sample
boldface font	Commands and keywords are in **boldface**. Also used for names of some GUI elements.	This is similar to the UNIX **route** command.
italic font	Arguments for which you supply values are in *italics*. Also used for publication names and for emphasis	See the *Cisco 6160 Hardware Installation Guide* for further details.
`screen` font	Terminal sessions and information the system displays are in `screen` font.	`Are you ready to continue?  [Y]`
`boldface screen` font	Information you must enter is in **`boldface screen`** font.	Login: **`root`** Password: **`<password>`**
^	The symbol ^ represents the key labeled Ctrl.	^D—The key combination in a screen display means hold down the Control key while you press the D key.
[ ]	Elements in square brackets are optional. Also used for default responses to system prompts.	[**no**] **offset-list** {**in** | **out**} *offset*
{x | y | z}	Alternative keywords are grouped in braces and separated by vertical bars.	**offset-list** {**in** | **out**} *offset*
< >	Nonprinting characters such as passwords are in angle brackets.	`DSLAM>` `Password: <cisco123>`
({ })	Indicate a required choice.	**offset-list** {**in** | **out**} *offset*
([{ }])	Indicate a required choice within an optional element.	[{*letter\number*}**Enter**]

Note Means *reader take note*. Notes contain helpful suggestions or references to material not covered in the manual.

Tip Means *the following information will help you solve a problem*. The tips information might not be troubleshooting or even an action, but could be useful information or information that might save time.

Caution Means *reader be careful*. In this situation, you might do something that could result in equipment damage or loss of data.

Warning **Means *danger*. You are in a situation that could cause bodily injury. Before you work on any equipment, you must be aware of the hazards involved with electrical circuitry and be familiar with standard practices for preventing accidents. To see translated versions of the warning, refer to the *Regulatory Compliance and Safety* document that accompanied the device.**

Related Documentation

A complete list of all DSL product related documentation is available on the World Wide Web at http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/index.htm.

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

You can access the most current Cisco documentation on the World Wide Web at the following sites:

- http://www.cisco.com
- http://www-china.cisco.com
- http://www-europe.cisco.com

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which is shipped with your product. The Documentation CD-ROM is updated monthly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual subscription. Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

http://www.cisco.com/go/subscription

Ordering Documentation

Most Cisco documentation is available only online at:

http://www.cisco.com/univercd/home/home.htm

You can order some printed Cisco documentation in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/cgi-bin/order/order_root.pl

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

We appreciate your comments and feedback about Cisco documentation. There are several ways to submit comments to Cisco.

- If you are reading Cisco product documentation on Cisco.com, you can obtain a comment form electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.
- You can e-mail your technical documentation comments to bug-doc@cisco.com.
- You can submit your comments by mail. Write to the following address:

  Cisco Systems
  Attn: Document Resource Connection
  170 West Tasman Drive
  San Jose, CA 95134-9883

- If you are a registered Cisco.com user, you can submit comments electronically.
  - To report problems, click **Feedback** in the toolbar at the top of any document web page, press the **Contact Cisco Now** button, and under Problem Type, select **CD/Online Documentation**. After you complete the form, click **Submit** to send it to Cisco.
  - To send your opinion of the DSL documentation, go to the following URL:

    http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/

    and click **here** at the top of the page in the sentence “Is this Cisco documentation helpful? Click here to give us your feedback.” This displays a Documentation Survey that you can complete and submit to Cisco electronically.

Obtaining Technical Assistance

Cisco provides Cisco.com as a starting point for all technical assistance. Customers and partners can obtain documentation, troubleshooting tips, and sample configurations from online tools by using the Cisco Technical Assistance Center (TAC) Web Site. Cisco.com registered users have complete access to the technical support resources on the Cisco TAC Web Site.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

- Streamline business processes and improve productivity
- Resolve technical issues with online support
- Download and test software packages
- Order Cisco learning materials and merchandise
- Register for online skill assessment, training, and certification programs

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

http://www.cisco.com/tac

All customers, partners, and resellers who have a valid Cisco services contract have complete access to the technical support resources on the Cisco TAC Web Site. The Cisco TAC Web Site requires a Cisco.com login ID and password. If you have a valid service contract but do not have a login ID or password, go to the following URL to register:

http://www.cisco.com/register/

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

http://www.cisco.com/tac/caseopen

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

The Cisco TAC Escalation Center addresses issues that are classified as priority level 1 or priority level 2; these classifications are assigned when severe network degradation significantly impacts business operations. When you contact the TAC Escalation Center with a P1 or P2 problem, a Cisco TAC engineer will automatically open a case.

To obtain a directory of toll-free Cisco TAC telephone numbers for your country, go to the following URL:

http://www.cisco.com/warp/public/687/Directory/DirTAC.shtml

Before calling, please check with your network operations center to determine the level of Cisco support services to which your company is entitled; for example, SMARTnet, SMARTnet Onsite, or Network Supported Accounts (NSA). In addition, please have available your service agreement number and your product serial number.

Overview of the CDM Graphical User Interface

This chapter provides a general overview for using the Cisco Digital Subscriber Line Manager (CDM) graphical user interface (GUI) to manage the Cisco DSLAM chassis and other network components. This chapter also describes how to navigate through the GUI.

This chapter includes the following sections:

Cisco DSLAM Hardware

CDM supports the following Cisco DSLAM chassis:

- 6015 (NI-2 cards only); support for both commercial and outside plant environment chassis
- 6100 (NI-1 and NI-2 cards)
- 6130 (NI-1 and NI-2 cards)
- 6160 (NI-2 cards only)
- 6260 (NI-2 cards only)

Refer to the Cisco publications at the following url for more detailed information about the individual DSLAM hardware:

http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/index.htm

Cisco DSL Manager Software Applications

The Cisco DSL Manager software consists of two applications:

- Cisco Element Manager Framework (Cisco EMF)—Designed for local and long distance telephone companies to manage their telecom switching and transmission equipment. Cisco EMF supports several different standards-based and proprietary management protocols. The Cisco EMF system architecture provides a distributed network management solution for management of large-scale networks.
- Cisco Digital Subscriber Line Manager (CDM)—A plug-in software module, referred to as an element manager, that adds custom graphical user interface (GUI) windows and modeling behavior to the standard Cisco EMF system. Element manager software allows you to manage specific types of network equipment, such as Cisco DSLAMs. Cisco EMF software is the framework that supports the functions of the CDM element manager.

Note For more detailed information about using Cisco EMF software, refer to the *Cisco Element Management Framework User Guide*.

Cisco EMF Software

You must install Cisco EMF before you can run CDM. Cisco EMF provides the commands, icons, and menus that you use to access the services available in CDM. Using CDM, you can configure the Cisco equipment that you want to manage on your network. Combined, Cisco EMF and CDM provide you with a visual representation of the Cisco DSLAM equipment on your network.

To run CDM, you must start Cisco EMF using the **cemf start** command. When Cisco EMF launches, CDM automatically starts. When you start a Cisco EMF session using the **cemf session** command, the Cisco EMF Launchpad window opens. You click the Viewer icon in the Launchpad to open the Map Viewer window where you can access all CDM menus and dialog boxes, or windows.

Note All users have access to the tools available in Cisco EMF. Not all users have access to CDM. The system administrator can restrict user access to CDM. When you log in to Cisco EMF, your access to the system is determined by your user name and password.

Cisco DSL Manager Software

This section provides an overview of the CDM software application and includes the following sections:

CDM is an element manager (plug-in module) for Cisco EMF. You can have a variety of element managers plugged into a single Cisco EMF application. For example, from one Cisco EMF application, you can monitor and manage the objects of a Cisco 6015, Cisco 6100, Cisco 6130, Cisco 6160, and Cisco 6260 chassis.

The CDM element manager is designed for network managers who are responsible for performing the following tasks:

- Deploying a DSLAM chassis
- Provisioning the DSLAM line cards
- Commissioning a deployed chassis to detect the line cards that are provisioned
- Constructing maps to display a GUI that represents the Cisco equipment on the network
- Accessing fault, configuration, performance, and security information by means of simple network management protocol (SNMP)
- Viewing alarms that CDM generates (alarms display as color-coded icons on the network maps)
- Creating and managing subscribers
- Adding subscriber and traffic descriptor profiles to manage lines and connections
- Creating and managing permanent virtual connections (PVCs) and soft PVCs
- Analyzing the performance statistics of the trunk port

Creating and Managing Database Files

From CDM, you can add elements (such as a Cisco DSLAM) and objects (such as NI-2 cards and line cards) to the database. You can modify and delete configuration information and update system software without disrupting traffic on the network. When you modify, delete, or add configuration information in CDM, the system sends the changes to the managed DSLAM.

The Cisco EMF and CDM applications exchange configuration data between the client workstations and the server as follows:

- The client communicates directly to the server, and requests any object information from the server.
- Most object information is retrieved from the DSLAM, and not stored locally in the server database.
- As you add, delete, or modify configuration information from a client workstation, the client instructs the server to perform all the updates.

Maintaining System Performance

The software stores a system log file (Syslog) and an event log file (EventLog) on the DSLAM that you can view from CDM. These files log all command line interface (CLI) commands that the DSLAM receives and all events that affect the device.

Additionally, CDM keeps an audit log for transactions that users make. This log reports affected attribute, time, date, and value changes. These changes are stored in the /opt/cemf/logs directory as audit files and are stored by CDM.

Each CDM process has a log file that stores process-generated messages. The log files are generally stored in the /opt/cemf/logs directory as .log and .old files. At installation, a system administrator may designate another directory to store these files. Usually, the transaction log file is stored in this same directory.

Viewing the System Log File

You can view or print system log information from the SysLog Messages window. The SysLog Messages window contains a list of network components from which you select to view error and status messages. Messages that may display in the SysLog Messages window for a component are alarms or loss of traffic notifications.

You can select a severity range for the events you want to view. The Debug severity level is the least severe type of message generated by the system, and Emergency is the most severe type of message. From the SysLog Messages window, you can select a single severity level for the error and status messages you want to view, or you can select a range of severity levels.

See the "Viewing and Configuring the System Log File" section on page 6-1 for more information about the system log file.

Viewing the Command History File

Each time you change a component configuration on the network, the system creates an entry in the Command History file. From the Command History window, you can view the details of each configuration entry, including information such as the event, the time the event occurs, the name of the logged-in user, the Internet address of the system that is making the request or the system about which information is being requested, and other information.

See the "Viewing and Configuring the Command Log Window" section on page 6-4 for more information about the command history file.

Configuring or Querying Network Components and Using Hierarchical Levels

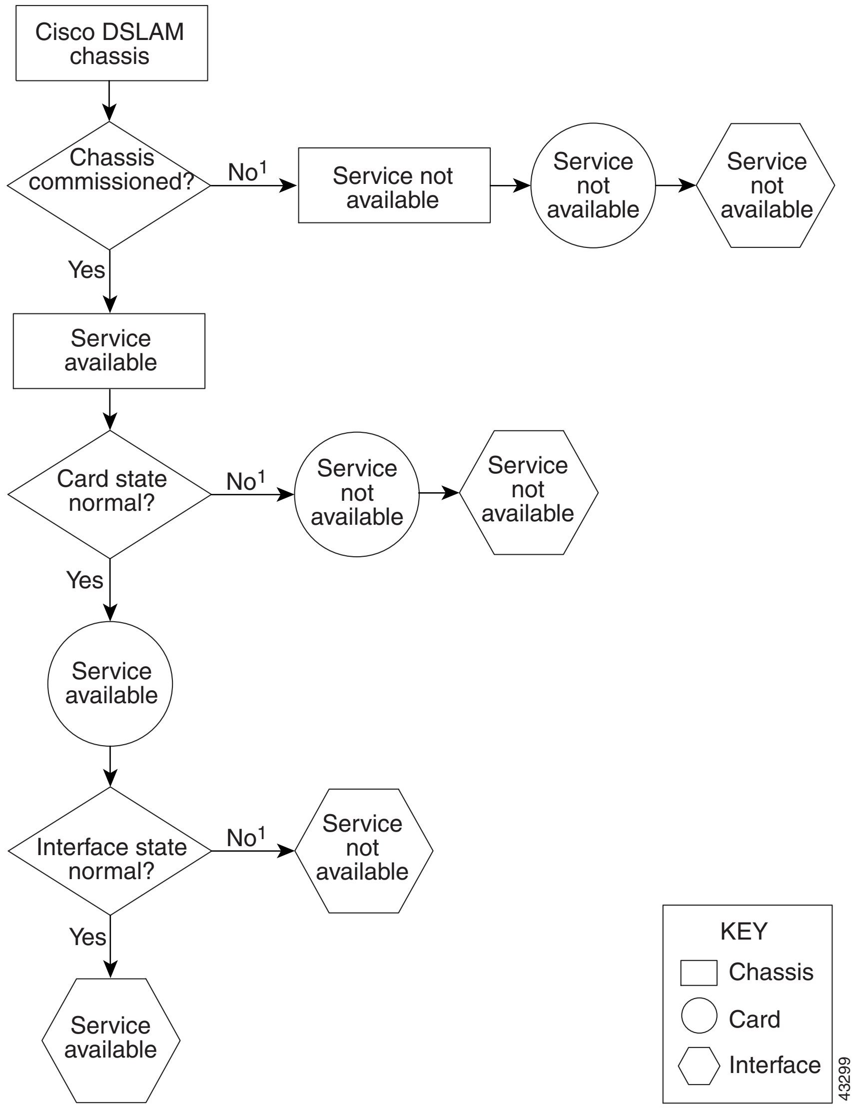
Through CDM, you can query or configure network components. You can manage these components by using a hierarchical structure. For example a site is a top-level hierarchy and contains DSLAMs. DSLAMs are the next level below site and contain cards. Cards are at the next level below DSLAMS and contain interfaces (or ports). Interfaces are at the next level below cards, and contain *x*DSL profiles and PVCs or SPVCs.

For network management, the state of the components also operate within a hierarchy—The lower level objects inherit the state, the availability of service, and the chassis or card with which they are associated.

For example, if you or the system decommissions a chassis, all cards and interfaces associated with that chassis become unavailable. If you or the system decommissions a card, all interfaces associated with that card become unavailable.

Figure 1-1 shows the hierarchy of the components, as well as how the state of each component affects the availability of its associated component. In this diagram, assume that the chassis and lower level objects are deployed.

Figure 1-1 Management Availability for Network Objects



1. No indicates any actual state other than Normal or Performanceloggingon

Identifying State Types

To identify the operational state of a selected component, look in the status bar on the bottom left corner of each window. The state of each component directly affects the operations you can perform on that component. By default, the window refreshes every 10 seconds and displays updated states.

The following sections provide a general overview of the states available in CDM:

Note For detailed information about element manager and object states, refer to the appendix about map states and icons in the *Cisco Element Management Framework User Guide*. This appendix provides descriptions of primary states, secondary states that display Open System Interconnection (OSI) icons above managed objects, and non-OSI icons.

Normal State

In the Normal state, CDM polls the network to detect the presence of objects. When an object enters the Normal state, CDM polls the object every 60 seconds to determine whether the object is present. An object is placed in the Normal state when you click the Commission button on that object. When you commission an object, you are requesting that the system place that object in the Normal state.

An object that is in the Normal state can be actively managed on the network.

Performanceloggingon State

When you start performance logging on an object, the state of that object changes from Normal to Performanceloggingon. The performanceloggingon state indicates that the selected card or interface has performance logging enabled. When you enable performance logging, the system collects performance data on the object. You can view the data in the Performance windows or right-click an object from the list box, and then choose Tools > Performance Manager from the object menu.

When an object is in the Performanceloggingon state, it can be actively managed on the network.

See Chapter 8, “Viewing Performance Data,” for more information about viewing performance data in the Performance windows.

Lostcomms or Discoverylostcomms State

If an object state is in lostcomms (lost communications) or discoverylostcomms, you are unable to query any of the displayed values. If you click a field in a window for any of the chassis objects when its state is in lostcomms or discoverylostcomms, the information does not display.

Decommissioned State

When you want to replace an existing card, or perform any kind of maintenance on an object, you should first decommission that object.

When you decommission an object, the following events occur:

- Active management is suspended
- All associated objects are decommissioned
- Polling on the object is suspended

Decommission buttons are located in certain windows, depending on the type of object you select. When you decommission a chassis, module, or line card, the system changes the state of all objects that are associated with this object to *decommissioned*. You must decommission a chassis, module, or line card before you delete it. (See the "Deleting Network Elements" section on page 2-49 for this procedure.) You cannot decommission interfaces, for example OC-3 or DS3 types of ports. However, if any object does not physically exist on the DSLAM, but exists in software such as a preprovisioned card, do not decommission it before you delete it from software.

Preprovisioned State

Preprovisioning applies to *x*DSL line cards only. After you insert a line card into a preprovisioned slot (preprovisioned with the same line coding), the state of the line card moves to a normal state. You do not need to commission this line card.

The Autodiscovery Process

The autodiscovery process detects any Cisco DSLAMs with either IP or SNMP identifiers. When you activate the autodiscovery function, the system detects a chassis and creates a chassis object. The software places that chassis object below the path that you specify in the Use Physical Path field in the Autodiscovery window. The software also creates a map of the chassis and its associated objects.

Autodiscovery can detect objects on more than one subnetwork by using multihop discovery. You can specify the physical location under which you want the software to create the discovered objects. You can also schedule multihop discovery to run at preset times. (Refer to the *Cisco Element Management Framework User Guide* for instructions on setting the schedules.)

Autodiscovery detects the presence of devices through the following processes:

- IP—Internet Connection Management Protocol (ICMP) pings are sent to IP addresses within a given IP address range. If a response is received on an ICMP ping, an object is created; if no response is received, no object is created.
- SNMP—SNMP get requests are sent to IP addresses in a given IP address range. Several SNMP community strings can be used so that equipment with different community strings are discovered in the same discovery session. Based on the SNMP information returned for devices, Cisco EMF decides whether the device is a DSLAM. If the device is a DSLAM, an object is created; if the device is not a DSLAM, no object is created.
- IP and SNMP—This is the default setting. In this process, ICMP pings are sent to find devices. If a device is found, SNMP get requests are sent and, based on the information they receive, Cisco EMF determines whether the device is a DSLAM. If the device is a DSLAM, an object is created; if the device is not a DSLAM, no object is created.

Refer to the *Cisco Element Management Framework User Guide* for detailed information about using autodiscovery.

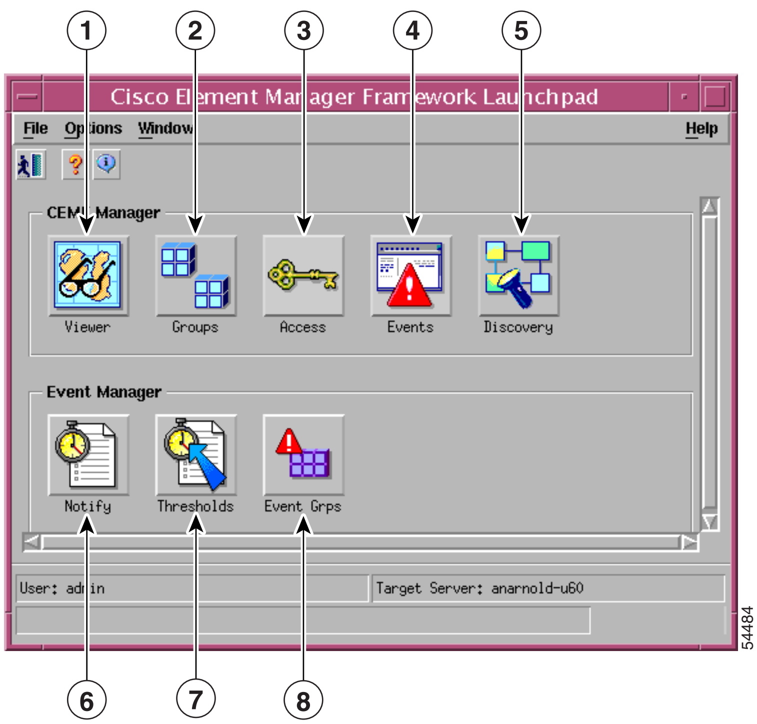
Using the Cisco EMF Launchpad

This section provides an overview of the Cisco EMF Launchpad and includes the following sections:

- Viewer Icon, page 1-9
- Groups Icon, page 1-10
- Access Icon, page 1-10
- Events Icon, page 1-11
- Discovery Icon, page 1-11
- Notify Icon, page 1-12
- Event Grps Icon, page 1-13

The Cisco EMF Launchpad, which is shown in Figure 1-2, is the first window that opens after you successfully start a Cisco EMF session. Throughout this guide, the Cisco EMF Launchpad window is referred to as the Launchpad. The Launchpad contains two areas—the CEMF Manager and the Event Manager.

Figure 1-2 Cisco EMF Launchpad Window



1	Viewer icon—Launches the Map Viewer	**2**	Groups icon—Launches the object group manager

3	Access icon—Launches the Access Manager	**4**	Events icon—Launches the Query Editor and the Event Browser
5	Discovery icon—Launches Autodiscovery	**6**	Notify icon—Launches the Notification Profile applications
7	Thresholds icon—Launches the Thresholding Regimes application	**8**	Event Grps icon—Launches the Event Groups applications

The icons that display in the Cisco EMF Launchpad window represent access to applications that are available with the standard Cisco EMF installation. Additional icons may appear if you install additional applications. Two methods are available from which you can launch an application:

- Click the icon located in the Cisco EMF Launchpad window.
- Choose the option from a menu. Access the menu by right-clicking a selected object, and then navigating to the appropriate option for the task you want to perform.

Note The first time you access the Launchpad window, your console must be set up to display sufficient colors. Otherwise, you may be unable to launch an application by clicking its icon. If you are unable to open an application by clicking its icon, try moving the Launchpad window to look for a dialog box that is open behind it. The following warning message displays in the dialog box, "There are insufficient colors available for CEMF client. Some applications may not display information correctly." You must click OK in the warning dialog box to launch an application.

The standard Cisco EMF application icons are shown in Figure 1-2.

The following sections briefly describe the icons that display in the Launchpad. Refer to the *Cisco Element Management Framework User Guide* for more detailed information about Cisco EMF applications.

Icons in the CEMF Manager Area

The icons in the CEMF Manager area are described in this section.

Viewer Icon

Click the Viewer icon, which is shown in Figure 1-3, to open the Cisco EMF Map Viewer window, through which you can view, build, and monitor your network by using graphical representations of network elements.

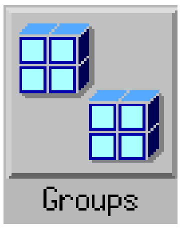
Figure 1-3 Viewer Icon

The Viewer icon is the primary entry point into CDM. When you open the Map Viewer window, you can monitor the status of all network elements or abstractions of elements that the network contains, and you can launch any additional applications from the Launchpad.

Groups Icon

Click the **Groups** icon, which is shown in Figure 1-4, to launch the Cisco EMF Object Group Manager window. You can also select **Groups** from an object menu from other Cisco EMF windows.

Figure 1-4 Groups Icon



You can use the Cisco EMF Object Group Manager, called Groups, to organize network elements into object groups. See the "Creating User Groups" section on page B-1 for how to set up user groups for CDM.

Note For more detailed information about this feature, refer to the chapter about the Object Group Manager in the *Cisco Element Management Framework User Guide*.

Access Icon

Click the **Access** icon, which is shown in Figure 1-5, to open the Cisco EMF User Access Control manager window.

Figure 1-5 Access Icon

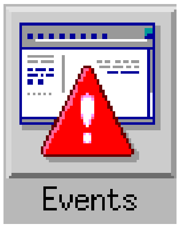
The Cisco EMF User Access Control feature allows system administrators to control user access to specific features of their system. Access control is important for security as well as efficient and effective network management. See the "Creating User Groups" section on page B-1 for instructions to customize user access in CDM.

Note For more detailed information about this feature, refer to the chapter about User Access Control in the *Cisco Element Management Framework User Guide*.

Events Icon

Click the Events icon, which is shown in Figure 1-6, to open a Query Editor window, from which you can specify alarm and event severity for monitoring alarms and events that occur within the system. These events display in the Event Browser window. See Appendix A, "Viewing Alarms and Events," for more information about using the Event Browser window.

Figure 1-6 Events Icon

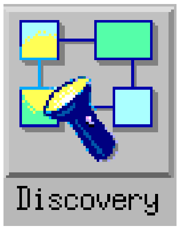


In Cisco EMF, when a condition or fault occurs on a managed object in the network, the system receives immediate notification. Being able to identify system events and quickly resolve them is one of the most important aspects of network service management. For example, a power supply fault in a chassis is a critical fault that might require an immediate field service call.

Discovery Icon

Click the Discovery icon, which is shown in Figure 1-7, to open the Cisco EMF Auto Discovery window. You can click this icon or you can select Discovery from an object menu to begin the autodiscovery process.

Figure 1-7 Discovery Icon



The Cisco EMF autodiscovery feature allows you to survey the network for IP and SNMP devices and create a managed object for each new device that it discovers. You can access Auto Discovery from the Cisco EMF Launchpad window or from an object menu.

Icons in the Event Manager Area

This section briefly describes the icons that display in the Event Manager area of the Launchpad.

Notify Icon

Click the Notify icon, which is shown in Figure 1-8, to launch the notification profile application.

Figure 1-8 Notify Icon

Cisco EMF uses notifications to inform operators of network events that it has monitored. You can set notification profiles to specify how notifications are collected. Refer to the chapter about notification profiles in the *Cisco Element Management Framework User Guide* for more detailed information.

Thresholds Icon

Click the Thresholds icon, which is shown in Figure 1-9, to launch the thresholding regimes application.

Figure 1-9 Thresholds Icon

A threshold regime is a set of threshold conditions for specified object attributes which, when breached, causes the software to run one or more notification profiles. Refer to the chapter about thresholding regimes in the *Cisco Element Management Framework User Guide* for more detailed information.

Event Grps Icon

Click the Event Grps icon, which is shown in Figure 1-10, to launch the event groups application.

Figure 1-10 Event Grps Icon

You can use the event groups application to organize network elements into event groups and view the status of these groups as scoreboards. Refer to the chapter about event groups in the *Cisco Element Management Framework User Guide* for more detailed information.

Navigating in CDM

CDM uses the familiar functions and menus that are found in most UNIX-based GUI products. This section describes the functions that are available in CDM and includes the following topics:

- Using Keyboard Commands, page 1-13
- Using the Right Mouse Button, page 1-13
- Using the Object Menus, page 1-19
- Using Other GUI Navigational Tools, page 1-24

Using Keyboard Commands

Certain keyboard commands are available in CDM. These commands serve as an alternative to mouse functionality. Table 1-1 shows the available keyboard commands and their descriptions.

Table 1-1 CDM Keyboard Commands

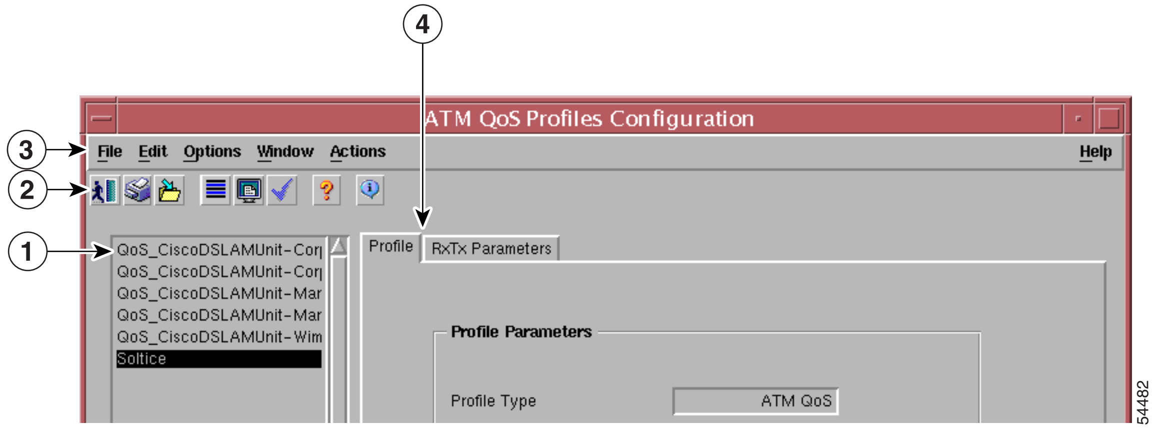
Keyboard Command	Use To…
Tab	Move among the fields in a window.
Arrow keys	Scroll through the text in a data entry field or through the values of a list box.
Alt key	Access a menu by entering the appropriate keyboard command. For example, to access the File menu using a keyboard command, press the Alt + F keys.

Using the Right Mouse Button

Cisco EMF and CDM provide right-click mouse functionality. Position the cursor over an object or an event listed in the Event Browser, and then right-click to view the menu options available for that object. This menu is referred to as the object menu throughout this guide. Once you access the object menu, you can use either mouse button to select the option you want.

The menu bar is located at the top of each window, as shown in Figure 1-11.

Figure 1-11 Example of CDM Window Showing the Menu Bar



1	List box entries	**2**	Toolbar
3	Menu bar	**4**	Tabs

Click the preferred menu from the menu bar to display the menu choices for that menu. You can also access a menu by entering the appropriate keyboard command. For example, to access the File menu with a keyboard command, simultaneously press the **Alt** and **F** keys. Refer to the section about shortcut keys in the "Welcome to Cisco Element Management Framework" chapter of the *Cisco Element Management Framework User Guide* for a list of keyboard shortcuts.

Note The menu choices that display in the Cisco EMF windows and CDM windows menu bar vary depending on the window from which you are viewing or configuring information. In addition, if a menu option is dimmed, the option does not apply to the active window (the window you are currently viewing or configuring).

The CDM menu bar menus are described in the following sections:

- File Menu, page 1-14
- Edit Menu, page 1-15
- View Menu, page 1-15
- Options Menu, page 1-16
- Window Menu, page 1-17
- Navigation Menu, page 1-17
- Actions Menu, page 1-17
- Help Menu, page 1-17

File Menu

The File menu contains choices for common operations such as Print, Save, and Close.

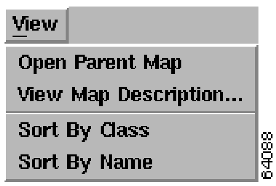
Edit Menu

The Edit menu contains choices for Copy Configuration, Copy Page Configuration, and Paste and Save Configuration. You can copy the configuration from one window and paste it into a different window to minimize duplicate data entry.

View Menu

The View menu, which is shown in Figure 1-12, is accessible in the Map Viewer window. You can use the View menu to open map views from within a map view, view text descriptions of the object you are viewing, and sort the contents of the object list box by class or name.

Figure 1-12 View Menu



The View menu choices are described in Table 1-2.

Table 1-2 View Menu Description

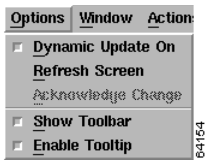
Menu Choice	Description
Open Parent Map	Open a parent map if you are viewing a window for an associated object. For example, if you are viewing a chassis (from the Map Viewer Component Managed view), you can select Open Parent Map to view the site map to which the chassis is associated. Or if you are viewing a line card, you can select the Open Parent Map option to view the chassis to which the line card is associated.
View Map Description	View the contents of the window in text format. For example, if you are viewing a chassis (from the Map Viewer Component Managed view), you can select View Map Description and a Map Description Text window displays the chassis configuration in text format.
Sort By Class	Sort the contents of the object hierarchy in the object list box by class. This means that the hierarchy is nonobject oriented—Shelf[1], cards, and then chassis.
Sort By Name	Sort the contents of the object hierarchy in the object list box by name. This means that the hierarchy is object-association oriented—Shelf, chassis, and then cards.

1. Cisco EMF automatically creates an object called a shelf when you deploy a DSLAM. The DSLAM becomes an object within a shelf.

Options Menu

You can use the Options menu, which is shown in Figure 1-13, to update configuration changes manually or to set the system to automatically update all configuration changes. You can also view or hide the toolbar, and enable or disable tooltips from the Options menu.

Figure 1-13 Options Menu



The Options menu choices are described in Table 1-3.

Table 1-3 Options Menu Description

Menu Choice	Description
Dynamic Update On	Set the system to automatically update the contents of the window each time you, or another user, make a change to the configuration. If a checkbox appears to the left of the option, the option is enabled.
Refresh Screen	Set the system to update the contents of the window *only* when you select this option. If you want the system to automatically update the contents of the window each time you, or another user, make a change to the configuration, enable the Dynamic Update On option.
Acknowledge Change	Click to acknowledge changes that occur in the window you are viewing or configuring. The default color for text in a window is black. However, if a change occurs to the window you are viewing, the text changes to blue. Often this choice is dimmed, as it appears in Figure 1-13, because no changes have occurred in the window.
Show Toolbar	View or hide the toolbar. If a checkbox appears to the left of the option, the toolbar is visible. If a checkbox does not appear to the left of the option, the toolbar is not visible. See the "Using the Toolbar" section on page 1-25 for more detailed information.
Enable Tooltip	View or hide tooltips. If a checkbox appears to the left of the option, a tooltip appears when you pause the pointer over an item in the window. If a checkbox does not appear to the left of the option, tooltips are disabled. The tooltips feature is enabled by default. When enabled, the tooltips feature displays a brief description of each icon when you place your cursor over the icon for a few seconds. **Note** The tooltips feature is especially helpful when you are setting subscriber properties and other configuration tasks within the windows in the GUI. As you set the values that are available in a window, the tooltips display the valid and available values for each setting.

Window Menu

The Window menu lists all of the windows that are open in CDM, with the exception of the active window. You can activate a nonactive window by selecting it from this list.

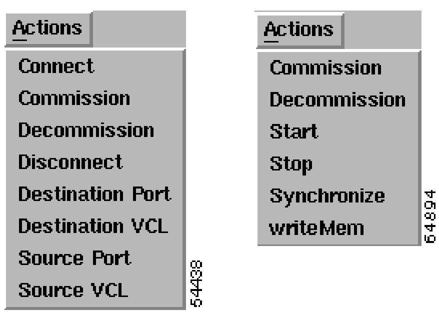
Navigation Menu

The Navigation menu choices are limited in this release and are dependent on which window you are in. For example, if you have the Subtend Configuration window open, the Navigation menu choices are Delete Subtend PVC and Add Subtend PVC.

Actions Menu

The menu choices in the Actions menu mirror the command buttons that appear in an active window. For example, if the active window displays a Commission and Decommission button, the Actions menu options are Commission and Decommission. Two examples of the Actions menu, the first from the ATM Connections Management window and the second from the Chassis Configuration window, are shown in Figure 1-14.

Figure 1-14 Examples of Actions Menus

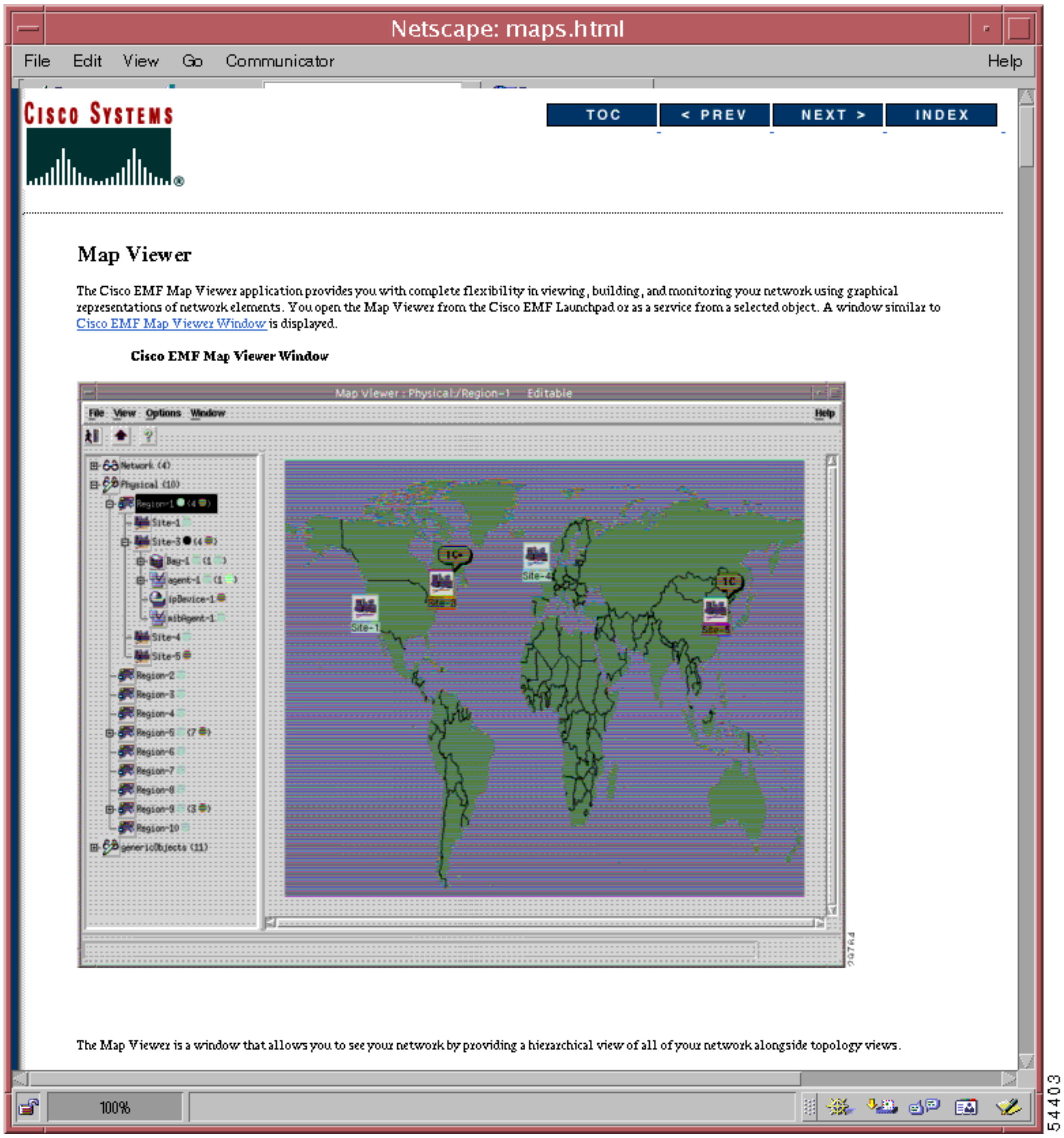


Help Menu

The Help menu and Icon Information options provide an online guide to Cisco EMF. Please consult the printed manuals available through the Cisco web site for help about CDM.

- Help—Contains information from the *Cisco Element Management Framework User Guide*. When you click the Help button, your Netscape browser opens to the Cisco Element Management Framework Help Page from which you can navigate to Cisco EMF help topics or Event Manager Applications Help topics. An example of this window is shown in the Figure 1-15.

Figure 1-15 Cisco EMF Help Page Window



- Icon Information—Contains descriptions of various events, states, severities, and so forth, as they relate to the icons in a window. For example, if a line card icon (in the Map Viewer window) contains diagonal lines, then the object is out of service. Or, if a solid line (link) connects two objects, the link is active. If a dotted line (link) connects two objects, the link is disabled.
- About—Lets you view the current version of Cisco EMF that is running on your system.

Note The first time you choose the About option, a Netscape license agreement window opens. Click the **Accept** button and the About Cisco EMF window opens.

By default, Netscape software is automatically downloaded when you install Cisco EMF software. The Cisco EMF/CDM Help system uses Netscape tools such as the search engine.

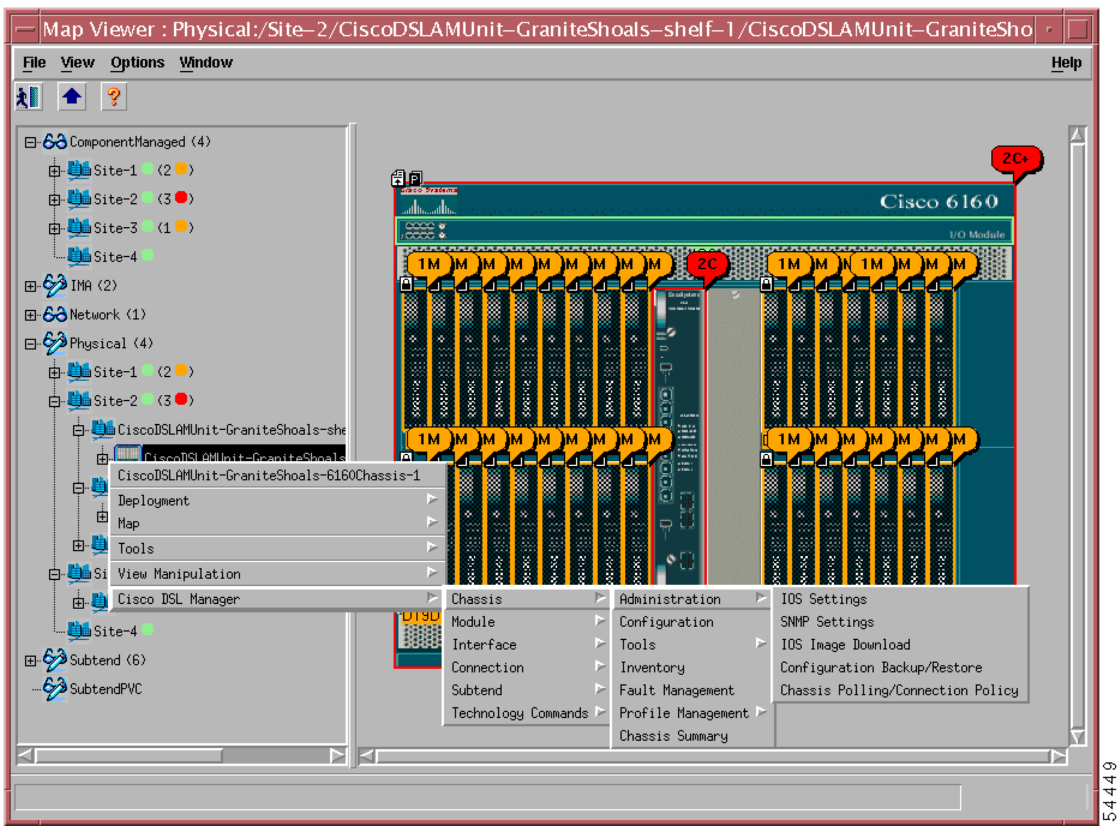
Using the Object Menus

This section describes the menus that open when you right-click over an object and includes the following sections:

- Deployment Menu, page 1-21
- Map Menu, page 1-21
- Tools Menu, page 1-22
- View Manipulation Menu, page 1-22
- Cisco DSL Manager Menu, page 1-23

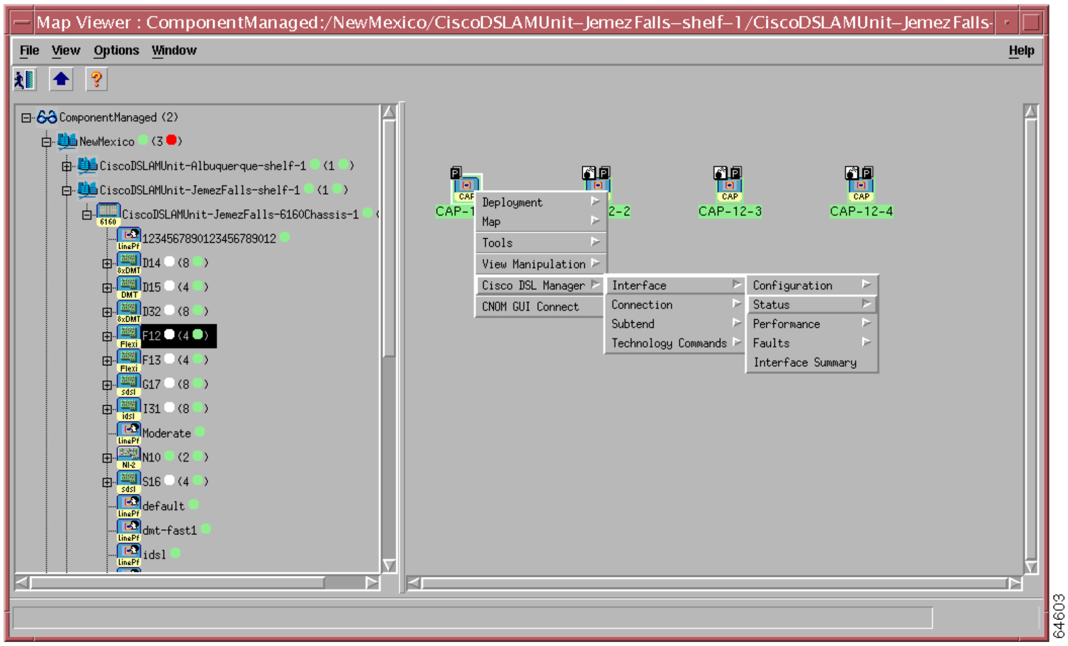
To access the CDM object menus, place your cursor over a CDM object on the left side of the Map Viewer window, over the chassis view, or over other object icons, then right-click. A single menu or a set of cascading menus open. An example of an object menu is shown in Figure 1-16.

Figure 1-16 Example of Opening the Set of Object Menus



You can also place your cursor over the graphical representation of the object on the right side of the Map Viewer window and right-click, as shown in Figure 1-17.

Figure 1-17 Map Viewer Window Showing Object Menus



Note In this user guide, instructions are given to access the object menus from the left side of the Map Viewer window. However, you can access these menus in the way that you find most convenient.

The choices on the object menus reflect the type of object from which you access the menu. Many of the tasks that you perform while using CDM are accessible through these cascading object menus.

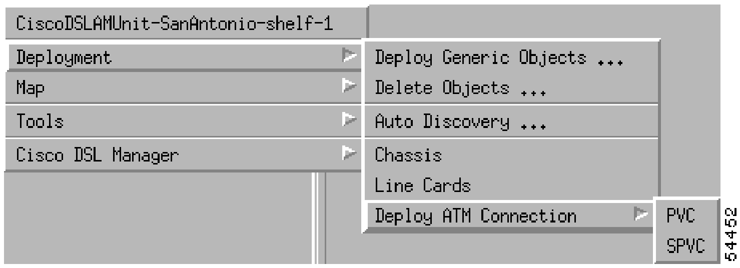
Choosing from an object menu opens a new window of that name. For example, if you right-click over a chassis object from the left side of the Map Viewer window, you can choose Deployment > Deploy Cisco DSLAM to open the Deployment Wizard window.

In this user guide, these menus are referred to as the object menu, even though the menu may include a set of several menus. These menus are described in more detail in the following sections.

Deployment Menu

To deploy a chassis or other object, you must access the Deployment menu, which is shown in Figure 1-18.

Figure 1-18 Deployment Menu



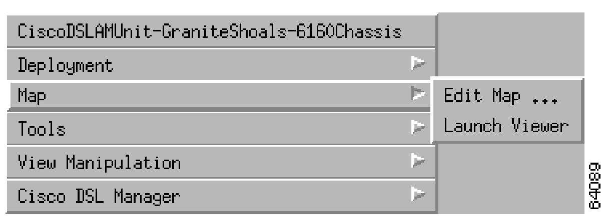
The Deployment menu has the following set of choices. The first three are generic to Cisco EMF, and the last three are specific to CDM.

- Deploy Generic Objects
- Delete Objects
- Auto Discovery
- Chassis
- Line Cards
- Deploy ATM Connection > PVC or SPVC

Map Menu

To access map functions in Cisco EMF, you must access the Map menu, which is shown in Figure 1-19.

Figure 1-19 Map Menu



The following choices are available from the Map menu:

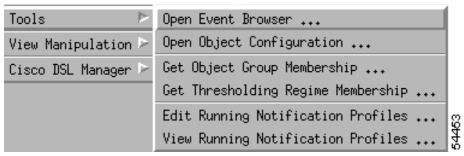
- Edit Map
- Launch Viewer

Note Refer to the *Cisco Element Management Framework User Guide* for more information about using these applications.

Tools Menu

To access Cisco EMF applications other than through the Launchpad, you can use the Tools menu, which is shown in Figure 1-20.

Figure 1-20 Tools Menu



From the Tools menu, you can choose from the following tasks:

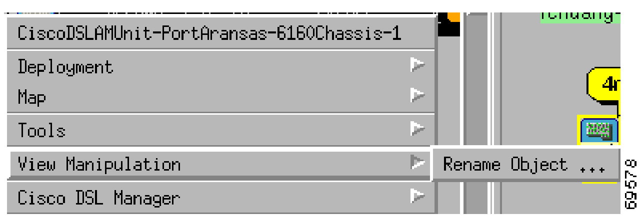
- Open Event Browser
- Open Object Configuration
- Get Object Group Membership
- Get Thresholding Regime Membership
- Edit Running Notification Profiles
- View Running Notification Profiles

View Manipulation Menu

The options that display from the View Manipulation menu depend on whether you open it from the chassis level or from the site level.

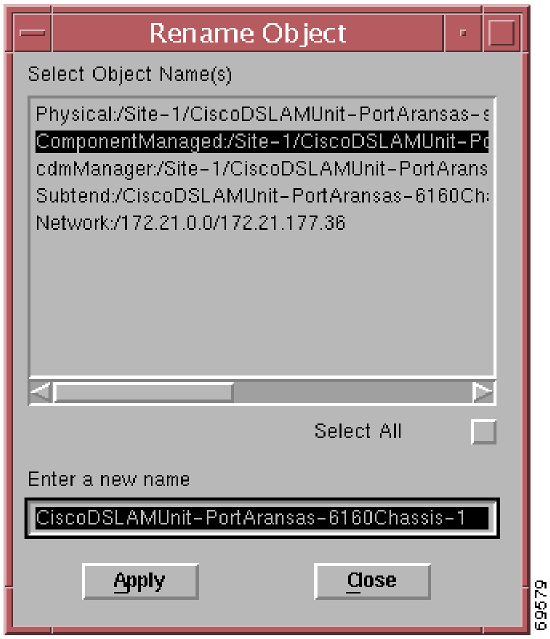
The View Manipulation window from the chassis level is shown in Figure 1-22.

Figure 1-21 View Manipulation Menu from Chassis Level



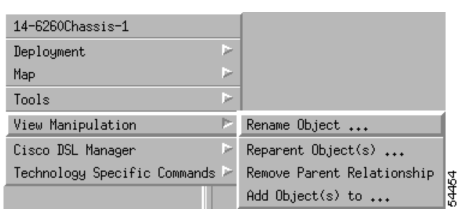
If you choose Rename Object, the Cisco EMF Rename Object dialog box opens, shown in Figure 1-22. Refer to the *Cisco Element Management Framework User Guide* for more information about renaming objects.

Figure 1-22 Rename Object Dialog Box



The View Manipulation menu from the site level is shown in Figure 1-23. Reparenting is not recommended because it may affect the integrity of your system data.

Figure 1-23 View Manipulation Menu from Site Level

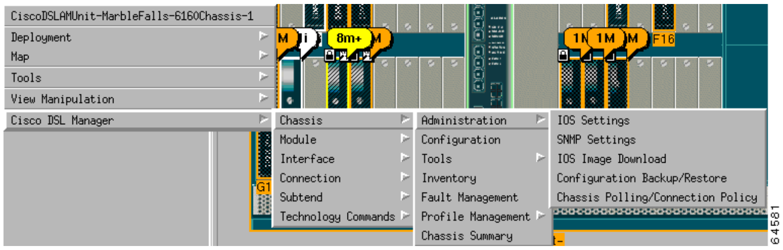


Cisco DSL Manager Menu

To access most of the windows through which you manage the Cisco DSLAM, you use the Cisco DSL Manager menu. This menu has several sets of menus from which you can choose many functions. The menus that open depend on what type of object you right-click to access the menus, that is, a chassis object, a module, an interface, a PVC, or a profile.

The Chassis Administration menu, which is shown in Figure 1-24, is an example of a Cisco DSL Manager object menu.

Figure 1-24 Cisco DSL Manager Menu—Chassis Administration



See Appendix C, "Using the Cisco DSL Manager Object Menus," for more detailed descriptions of all of the Cisco DSL Manager object menus.

Using Other GUI Navigational Tools

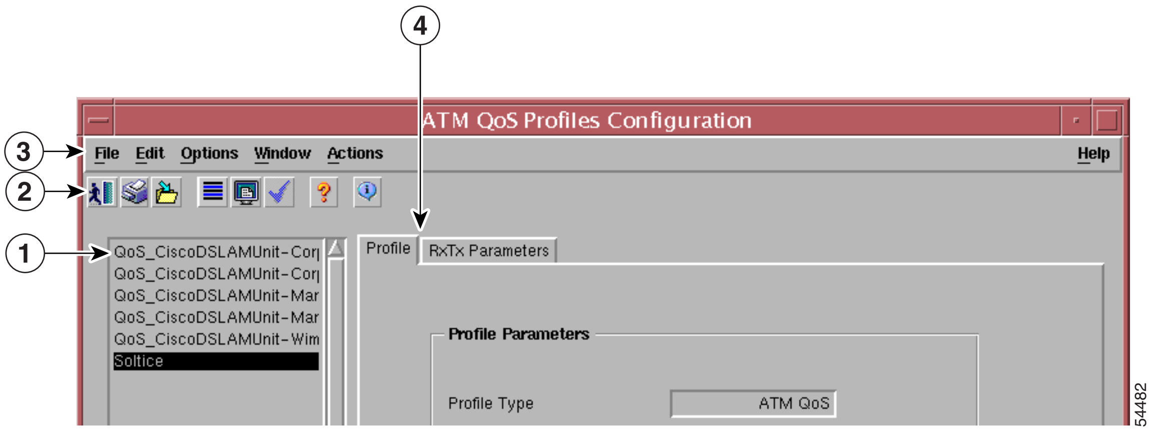
This section describes other navigational tools that you can use to perform tasks in CDM and includes the following topics:

- Using Tabs, page 1-25
- Using the Toolbar, page 1-25
- Entering Text into Fields and Using the Down Arrow, page 1-26
- Using the List Box Entries, page 1-26
- Using Buttons to Initiate Commands, page 1-26
- Viewing the Status Bar, page 1-27
- Understanding Informational Dialog Boxes, page 1-28

Using Tabs

Some windows have several sections that are separated by tabs. An example of tab structure is shown in Figure 1-25.

Figure 1-25 Example of a CDM Window Showing Tabs



1	List box entries	**2**	Toolbar
3	Menu bar	**4**	Tabs

Tabs separate related information when more information is required than can fit in a single window. Some windows have only one tab, which allows for development of new features in future releases of the software.

Using the Toolbar

The CDM toolbar (see Figure 1-25) is located directly below the menu bar, contains tool icons and provides quick access to CDM commands. You can use the tools in the toolbar to perform common functions such as close, print, save, update, and so forth. Additional tools allow you to access detailed information about a selection in the active window.

The tools that display in the toolbar depend on which window is active. If a tool is dimmed, it is not accessible from the active window. You can also disable the toolbar so that it does not display in the window.

To enable and disable the toolbar, choose **Options > Show Toolbar**.

To choose a tool from the toolbar, click once on the tool.

For a description of a tool, pause your cursor over the tool in the toolbar. A tooltip appears that describes the use of the tool.

Note In many of the CDM GUI windows, you can click the Save icon that is located in the toolbar to save any changes that you make in the window. Throughout this guide, instructions to click Save refer to clicking this Save icon in the toolbar.

Entering Text into Fields and Using the Down Arrow

To enter data in text fields, place your cursor in the field and enter the information by using your keyboard. Some text fields also provide a down arrow that you can click to display a set of valid options.

Using the List Box Entries

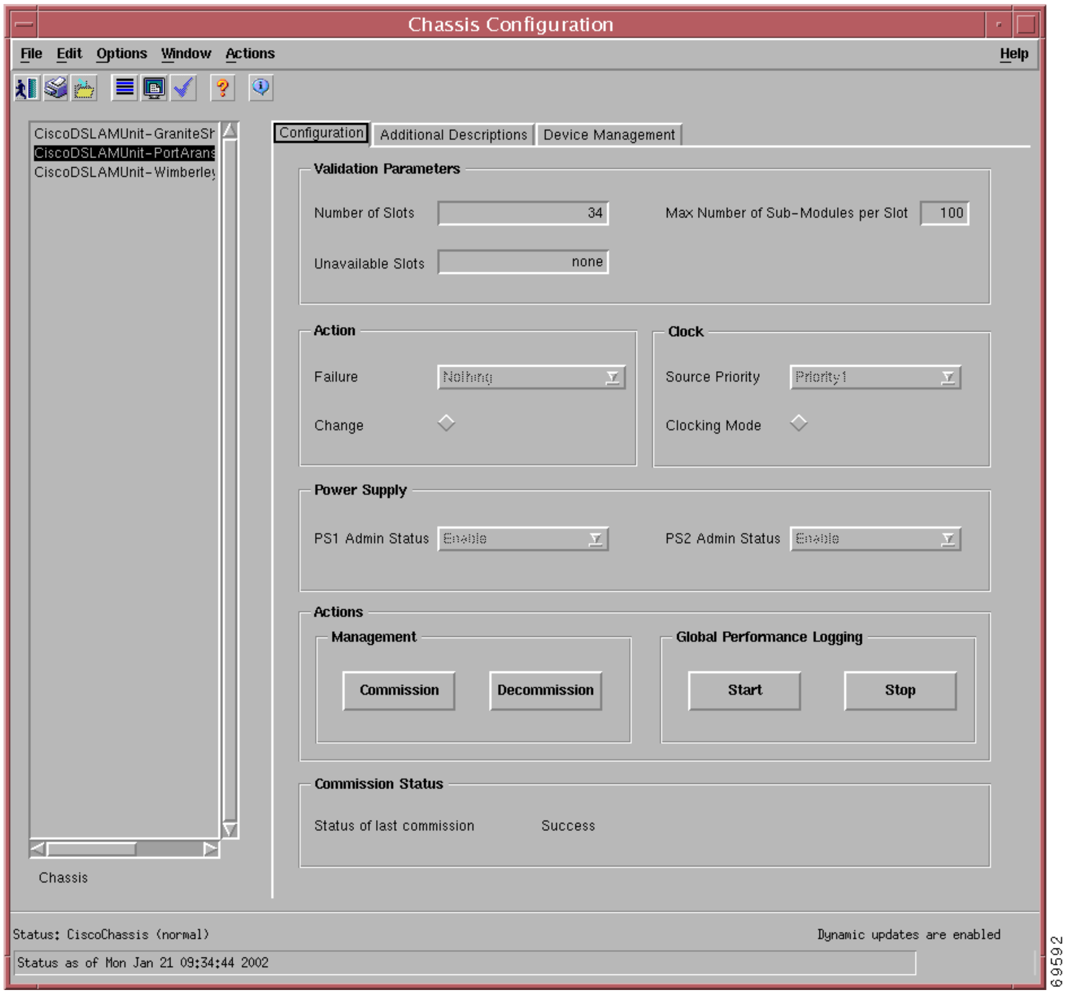
Most windows include a list box, which is shown in Figure 1-25 on page 1-25 on the left side of the window. When you select an object in the listbox, it is highlighted. The data about that object displays on the right side of the window, or you can set data for that object on the right side of the window.

Using Buttons to Initiate Commands

Buttons that initiate commands appear in windows from which you can configure or update information. The command buttons that appear depend on the window you are viewing or configuring.

For example, if you want to commission a chassis, select the chassis and navigate to the Chassis Configuration window, which is shown in Figure 1-26. Select the object or objects that you want to commission from the list box, and then click the **Commission** button.

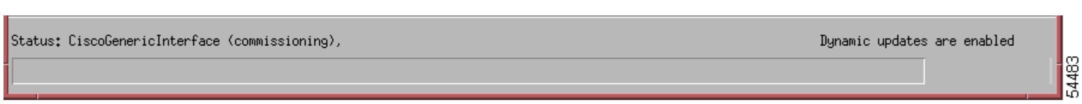
Figure 1-26 Chassis Configuration Window



Viewing the Status Bar

CDM displays a status bar, which is shown in Figure 1-27, at the bottom of a window. You can view system or network information in real time by reading the information in this status bar. CDM automatically updates the information in the status bar as you modify configuration parameters or send data changes to the node.

Figure 1-27 Status Bar Sample

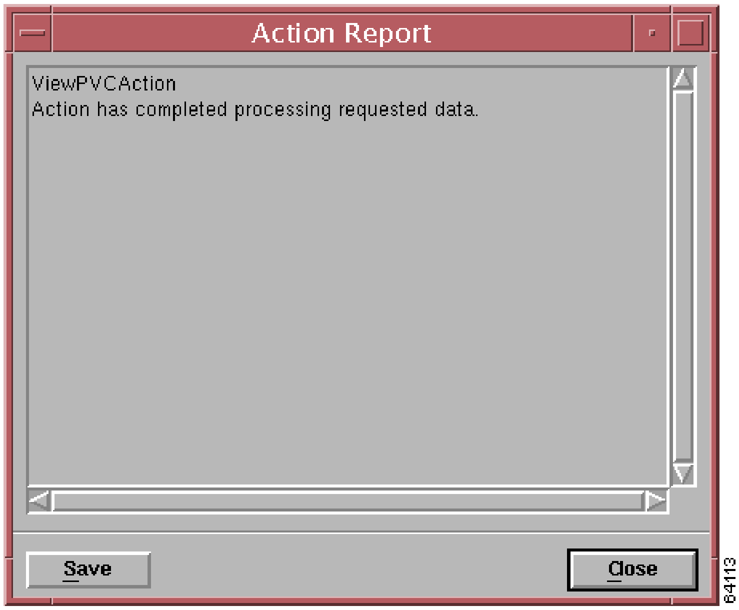


Understanding Informational Dialog Boxes

Most of the interfaces in the CDM GUI are referred to as windows. However, CDM also contains several dialog boxes that provide information about the success or failure of an action, or that ask you to confirm whether you want to proceed with an action. These dialog boxes include the Action Report dialog box, Prompt dialog box, Error dialog box, Notification dialog box, and so forth.

The Action Report dialog box generally informs you whether CDM successfully completed an action or process. An example of an Action Report dialog box is shown in Figure 1-28.

Figure 1-28 Example of an Action Report Dialog Box



The Prompt dialog box, which is shown in Figure 1-29, issues prompts from CDM.

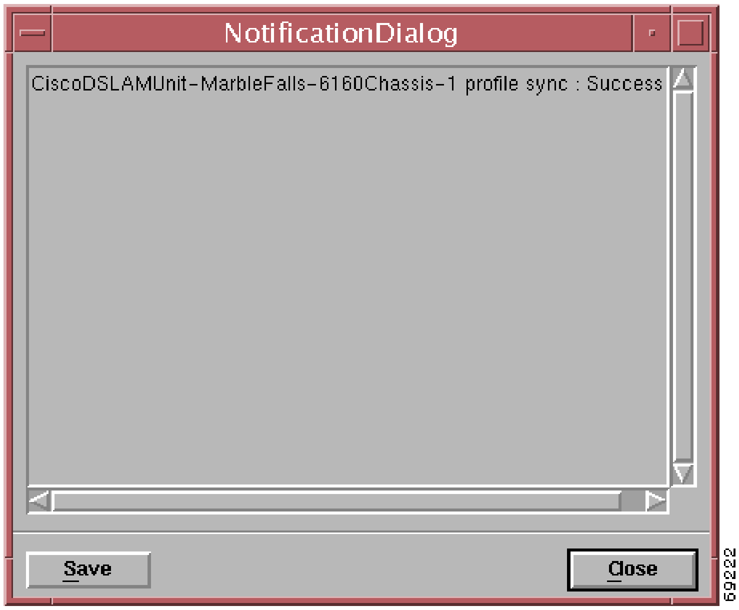
Figure 1-29 Example of a Prompt Dialog Box

The Error dialog box displays error messages. An example of an Error dialog box is shown in Figure 1-30.

Figure 1-30 Example of an Error Dialog Box

The Notification dialog box, which is shown in Figure 1-31, notifies you about certain processes.

Figure 1-31 Example of a Notification Dialog Box



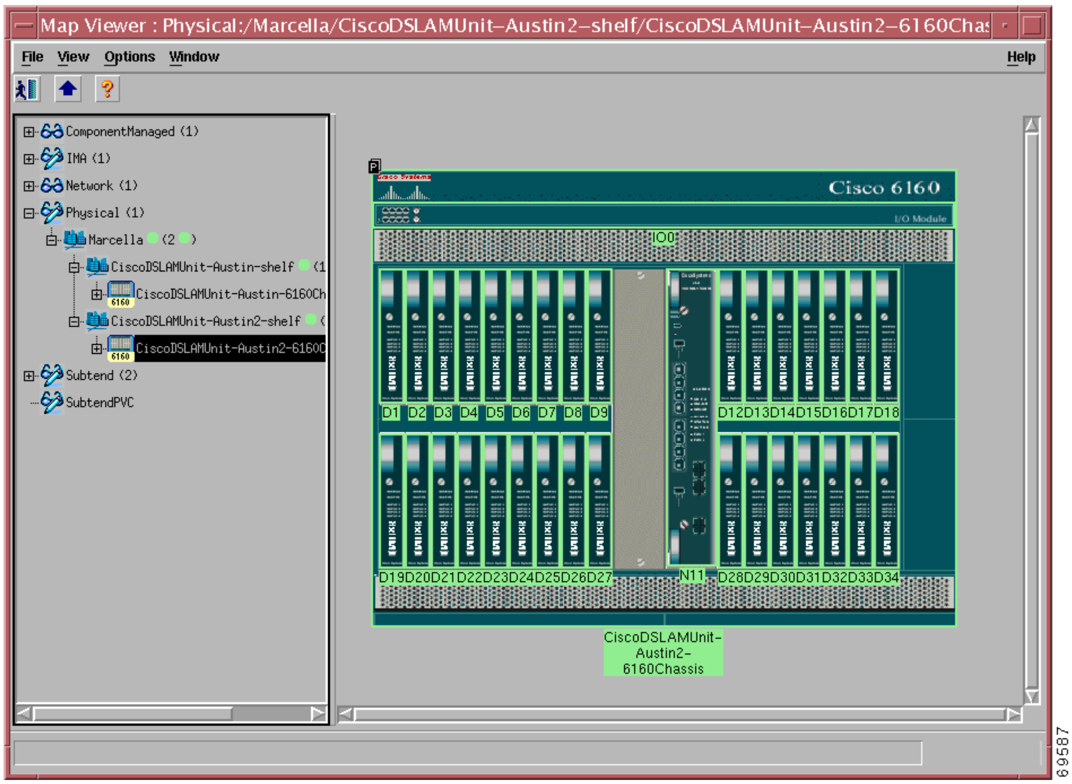
Other dialog boxes may open for which you click Yes or No. An example of this type of dialog box is shown in Figure 1-32.

Figure 1-32 Example of a Yes/No Dialog Box

Displaying Objects in CDM

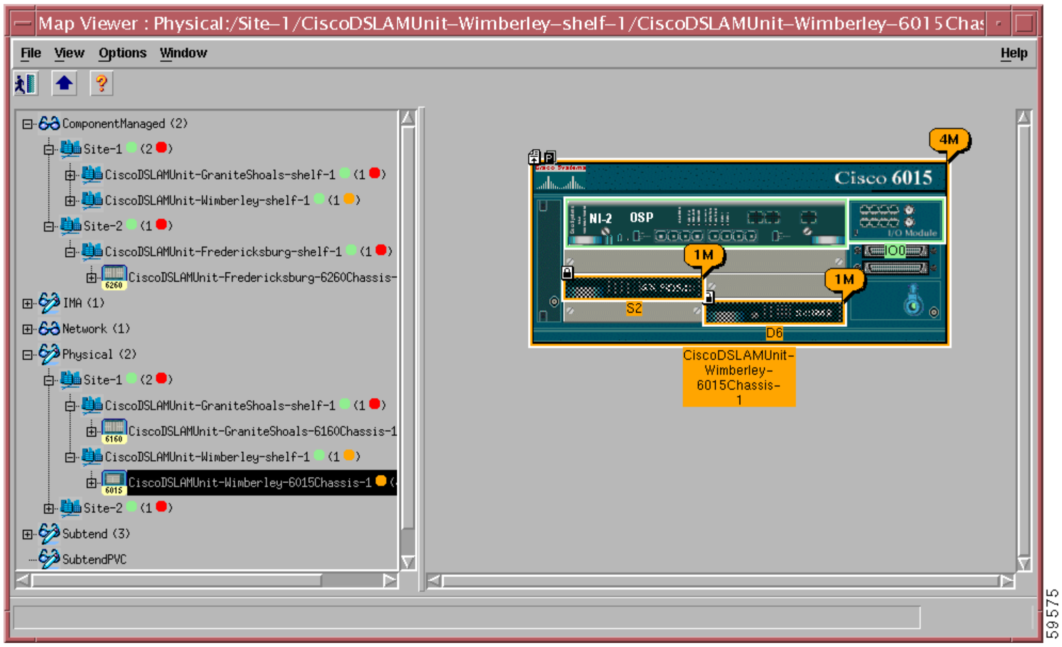
You can navigate through the Cisco EMF and CDM GUI by using graphical images and icons. To view or configure objects on your network, you should use the Physical hierarchy view or the Component Managed view, which are shown in Figure 1-33. The hierarchy views are located on the left side of the Map Viewer window. For more detailed information about the hierarchy views, see the "Using the Map Hierarchy Views" section on page 1-33.

Figure 1-33 Cisco DSLAM Chassis View



The graphical representation of a specialized module, such as the NI card for the Cisco 6015 OSP DSLAM, displays on the chassis view. See Figure 1-34. See the "Graphical Objects" section on page 1-33 for more information about the graphical objects that display on the chassis view.

Figure 1-34 Cisco 6015 OSP DSLAM Chassis View



Note For more information about the informational balloons that appear above the line cards in the chassis view, refer to the section about graphical cues in the *Cisco Element Management Framework User Guide*.

When you select an object such as a chassis, card, or interface from the cdmManager list, a graphical image of the object displays on the right side of the window. Figure 1-33 shows an example of a Cisco 6160 chassis image after you select the chassis from the hierarchical list on the left side of the window, and Figure 1-33 shows an example of a Cisco 6015 OSP chassis image.

To view or configure objects in CDM, follow these steps:

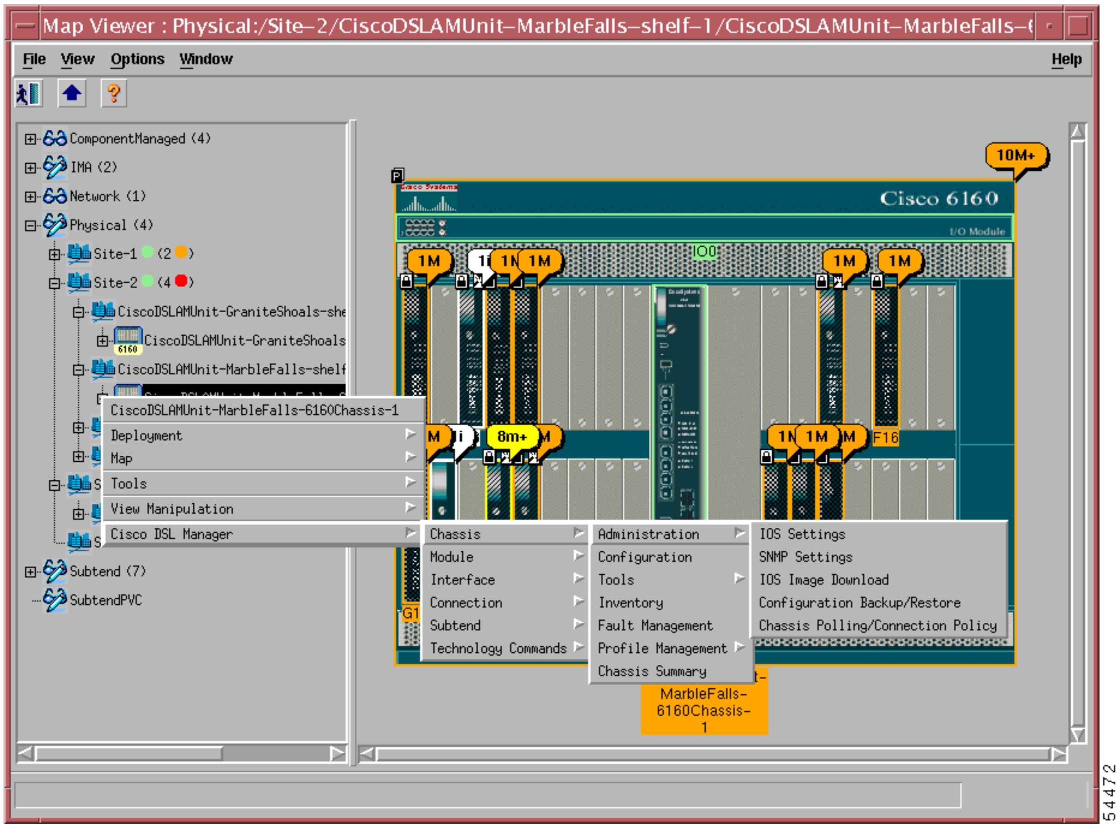
Step 1 Click the **Viewer** icon in the Launchpad to open the Map Viewer window, which is shown in Figure 1-33.

Step 2 Expand the hierarchy on the left side of the window, as follows, and select a chassis:

To expand the hierarchy, click the "**+**" next to the managed element name. A graphical image of the chassis displays on the right side of the window when you click the icon for that chassis, as shown in Figure 1-33. You can continue to expand the hierarchy by clicking the "**+**" next to the object name. You can also right-click an object, such as an NI-2 card or line card, in the chassis image on the right side of the Map Viewer window to display the menu options that are available for the selected object.

Figure 1-35 shows an example of an object menu.

Figure 1-35 Example of an Object Menu

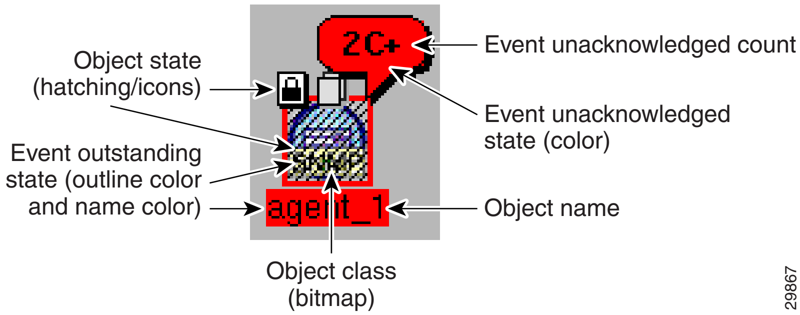


Step 3 Choose an option from the menu to view or configure the object on the network.

Graphical Objects

Graphical objects display additional icons on top of the existing object icons that the Map Viewer displays. The additional icons provide information such as the state of the object or the event status. See Figure 1-36.

Figure 1-36 Information that Displays on an Object



Note Events shown visually are the most severe.

A telecom graphical object represents a network element such as a node, shelf, shelf item, or link. Each object provides graphical cues that supply information about the associated network element of an object. This information can be structural, such as a network element name, or the information can be about states and events, such as out of service.

Note For more detailed information about the state and class information that an object displays graphically, refer to the section in Chapter 3 about graphical cues in the *Cisco Element Management Framework User Guide*.

Using the Map Hierarchy Views

This section describes the hierarchical map views and includes the following topics:

- Component Managed View, page 1-36
- IMA Hierarchy View, page 1-37
- Network Hierarchy View, page 1-37
- Physical Hierarchy View, page 1-39
- Subtend Hierarchy View, page 1-40
- Subtend PVC Hierarchy View, page 1-41

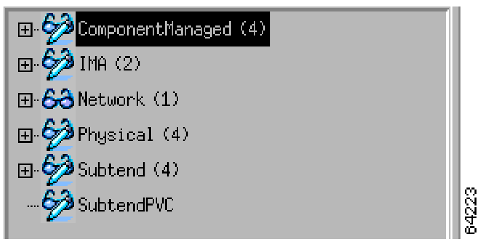
The map hierarchy view, on the left side of the Map Viewer window, models the hierarchical relationships between objects, both physical and logical. Objects are organized into different views and can exist in multiple views simultaneously by reference. Each object can have a number of parent and children objects. You can access CDM objects by navigating through one of the views to find the object. Each view represents a different way of containing and grouping objects.

When you open the Map Viewer window, you can monitor the status of all network elements or abstractions of elements that the network contains. The Map Viewer window is divided into two sections. The left side displays objects in a hierarchical map format. The graphical representation of an object that you select on the left displays on the right side of the window.

To resize the hierarchy and map areas, position your cursor over the boundary, and click and drag the boundary. You can view all information on the left and right sides of a window by using the horizontal and vertical scroll bars.

The top level CDM map hierarchy view is shown in Figure 1-37.

Figure 1-37 Top Level CDM Map Hierarchy View



The names that display at the top level (see Figure 1-37) are specific to Cisco EMF or to CDM. The standard Cisco EMF views are the Network and Physical views. All other views are specific to the CDM. You can accomplish most CDM-specific tasks by using the Physical or Component Managed view, through which you can look at physical maps of each Cisco DSLAM chassis. You can access the object menus for each managed object by right-clicking an object.

CDM has the following map hierarchy views:

- Component Managed view
- IMA view (pertains specifically to 6015 and 6160 DSLAMS with NI-2 modules)
- Network view
- Physical view
- Subtend view
- Subtend PVC view (this is the only view in which you can delete subtend PVCs.

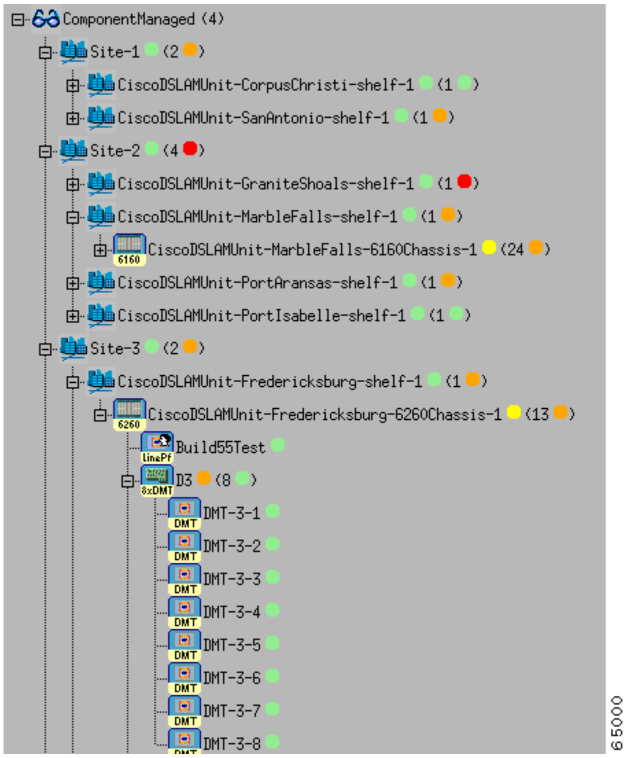
If you also install the CDM NI-1 element manager, the following hierarchy views display above the NI-2 hierarchy views:

- c61xxChassisView
- C6100v30Mgr

The map hierarchy views that are relevant to the Cisco NI-1 DSLAMS are described in the *Cisco DSL Manager NI-1 User Guide*.

An example of a hierarchy view, the Component Managed hierarchy view, is shown in Figure 1-39.

Figure 1-38 Component Managed Hierarchy View



In the hierarchy views, you see colored circles next to each object. The first circle that displays next to an object represents the highest level of alarm for that object. For example, if there is no alarm on that object, the circle is green for normal (see Table 1-4). The number and second circle that display in parentheses next to the object indicate the number of objects that are managed by that object and the highest severity level of alarms on any of those objects. So, if there is a 13 and a red circle, there are 13 objects associated with this object and there is a critical alarm on at least one of these subordinate objects.

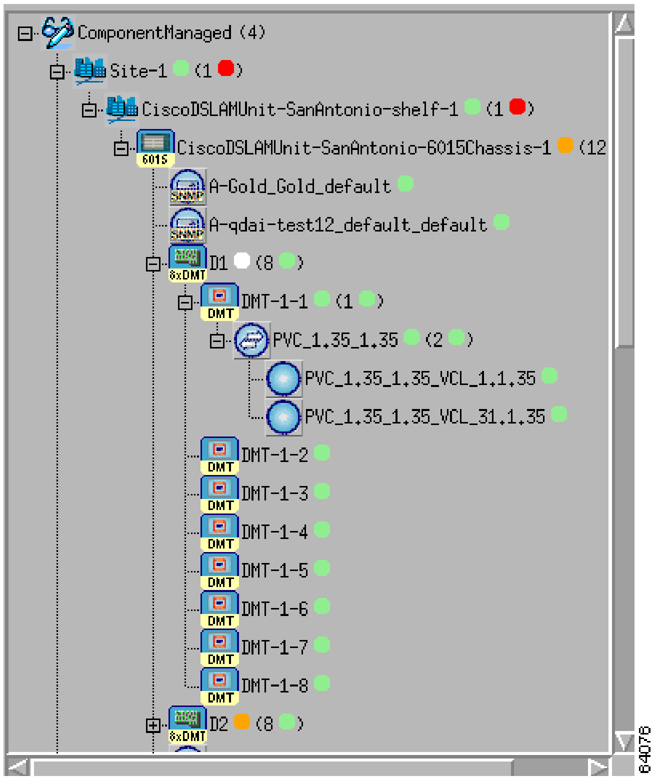
Table 1-4 Severity Colors

Color	Severity of Alarms
Red	Critical
Orange	Major
Brown	Moderate
Yellow	Minor
Cyan	Warning
Green	No alarms (normal)
Blue	Card decommissioned or not installed
White	Informational
Dark Green	Preprovisioned

Component Managed View

The Component Managed hierarchy view is shown in Figure 1-39.

Figure 1-39 Component Managed Hierarchy View



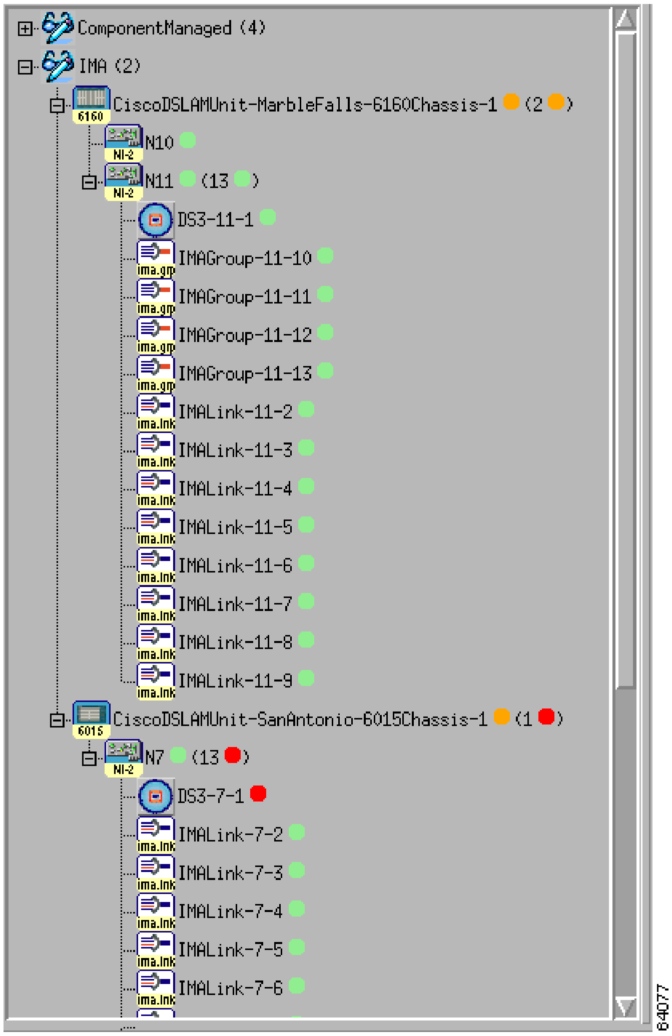
The Component Managed view is a superset of the Physical view (see the "Physical Hierarchy View" section on page 1-39). This view displays PVCs and SPVCs as children of the DSL line interface under which they are created and displays ATM QoS profiles as children of the DSLAM chassis object, as well as the details that display in the Physical view.

The difference between the Physical and Component Managed views is that when you click a chassis object from the Physical view, on the left side of the Map Viewer window, the GUI displays a bitmap representation of that chassis and its line cards on the right side of the Map Viewer window.

IMA Hierarchy View

The IMA hierarchy view displays IMA links that make up an IMA group on Cisco 6015 and Cisco 6160 DSLAMS. An example of this view is shown in Figure 1-40.

Figure 1-40 IMA Hierarchy View



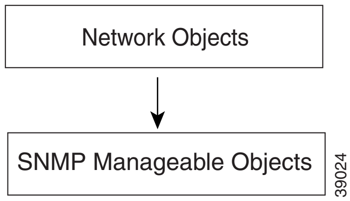
Network Hierarchy View

The Network hierarchy view represents the network devices within their respective networks and subnetworks.

The autodiscovery process uses the Network hierarchy view to determine which devices CDM has already added to the system, which prevents autodiscovery from trying to discover the same device multiple times. The Network hierarchy view is a standard view within the Cisco EMF software application.

The Network view displays all IP devices under their parent network. This view provides a logical layout of the network structure. It does not provide topology information. A diagram of the Network view is shown in Figure 1-41.

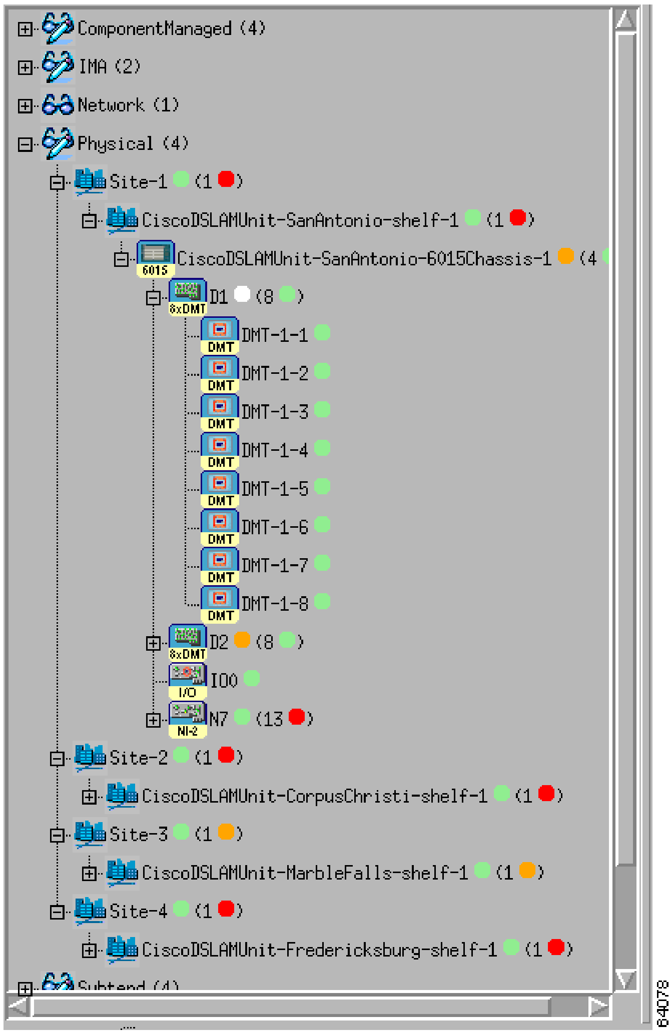
Figure 1-41 Diagram of Network Hierarchy View



Physical Hierarchy View

The Physical hierarchy view, which is shown in Figure 1-42, reflects the physical relationship of objects. From this view, you can drill down to specific interface icons to view the ports that are contained within each module.

Figure 1-42 Physical View



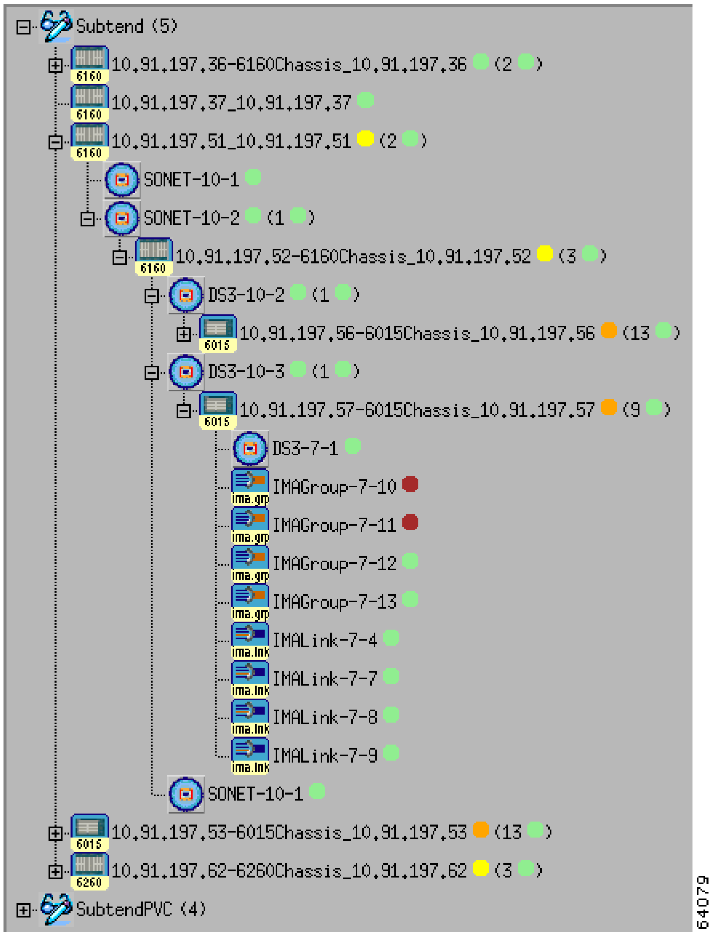
The Physical hierarchy view is common to Cisco EMF. Subscriber and pool information does not display from the physical map. Sometimes it is more convenient to work within the Physical view, but that is a matter of personal preference. The Physical view holds location information for all equipment in the network. In this view, relationships are defined based on the physical containment position of each object.

You can click a chassis object from the Physical view on the left side of the Map Viewer window. When you do, the GUI displays, on the right side of the Map Viewer window, a bitmap representation of that chassis and its line cards.

Subtend Hierarchy View

The Subtend hierarchy view, which is shown in Figure 1-43, displays subtended DSLAMs in hierarchical order.

Figure 1-43 Subtend Map Hierarchy View

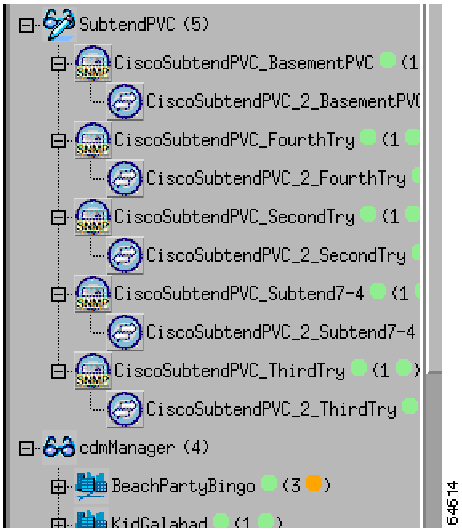


The Subtend View contains each chassis and its network interface ports. After CDM discovers the subtend topology, this view displays the connections between trunk and subtend network interface ports of DSLAMs in a subtended relationship. The trunk port of a subtended (child) DSLAM is connected to the subtend port of a subtending (parent) DSLAM. In this illustration, the DS3-11-1 is the trunk for the IMA groups and IMA links. For more detailed information about these relationships, see Chapter 5, "Configuring Subtend Configurations."

Subtend PVC Hierarchy View

The Subtend PVC Hierarchy view, which is shown in Figure 1-44, displays the subtend PVCs that have been created within subtended DSLAMs.

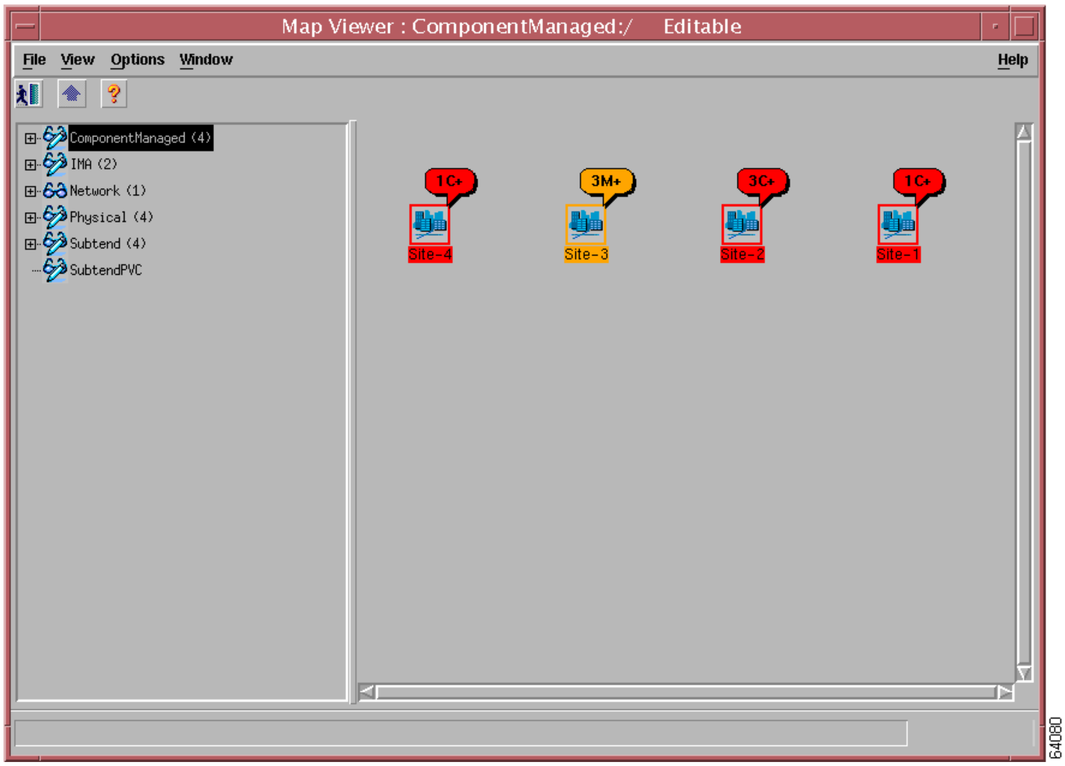
Figure 1-44 Subtend PVC Hierarchy View



Viewing the Map Viewer Window and the Cisco DSLAM Chassis

When you first open CDM by clicking the Viewer to open the Map Viewer window, the window that is shown in Figure 1-45, opens.

Figure 1-45 Map Viewer Window Opening View



The Map Viewer window uses graphical representations of network elements, through which you can view, build, and monitor your network. Examples of the Map Viewer window showing the graphical representation of a chassis are shown in Figure 1-46 and Figure 1-47. This is the view that you see after you have deployed the chassis and modules (line cards), and commissioned them. (See Chapter 2, "Getting Started Using CDM," for these procedures.)

Figure 1-46 Map Viewer Window Showing Chassis View

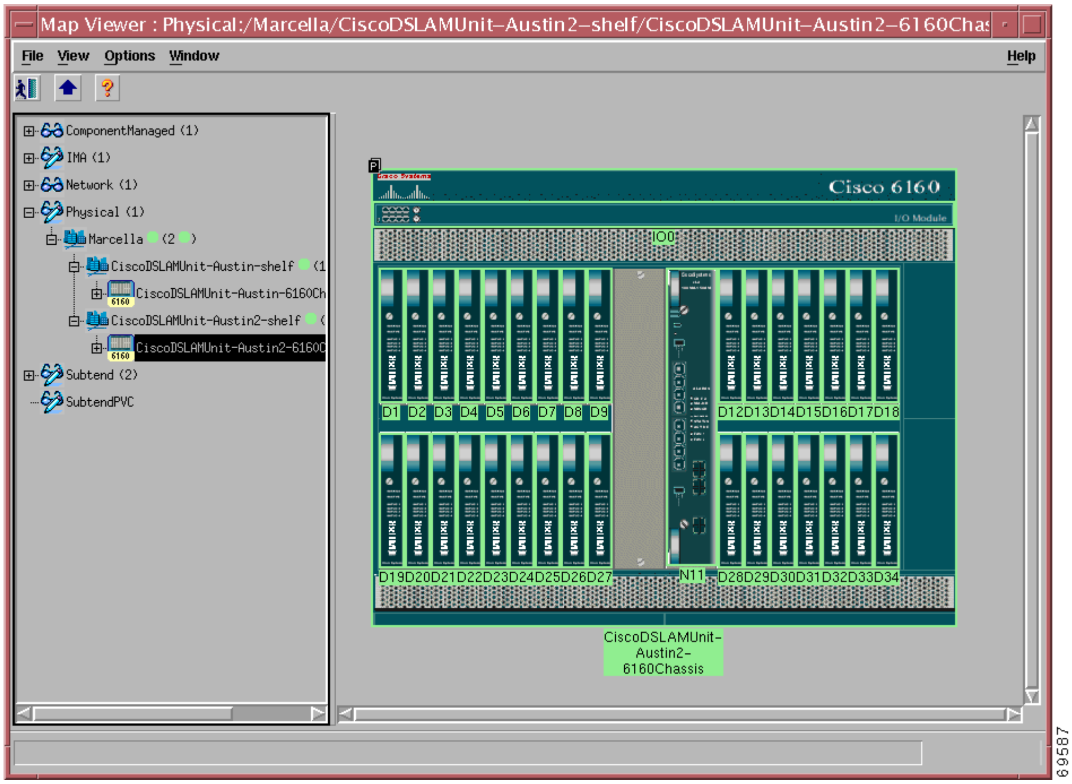
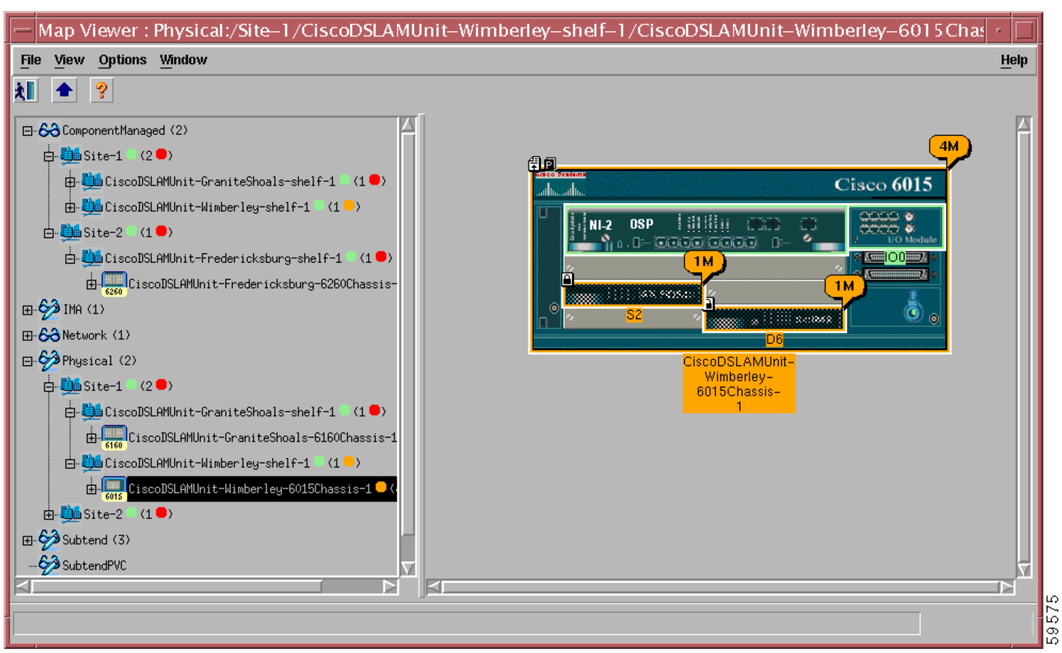


Figure 1-47 Cisco 6015 OSP DSLAM Chassis View



As CDM deploys and synchronizes a chassis, arrows that point up appear on each module. When the arrows disappear, that is an indication that CDM has deployed and synchronized that module.

Each module on the chassis view is outlined in a color or uses some other graphical notation to help you identify the object state and current alarm status, as follows:

- Red = critical alarm
- Orange = major alarm
- Yellow = minor alarm
- White = information
- Green = normal
- Hatched (///) = decommissioned
- Object Balloon = information

Note Refer to the "Graphical Cues" and the "Informational Icons" sections of the *Cisco Element Management Framework User Guide* for more detailed information about Cisco EMF graphical cues, including alarm and object status, that you see in the CDM GUI.

Viewing CDM Alarms and Events

CDM supports a number of alarm sources, including SNMP traps and SNMP alarm tables for Cisco chassis. In addition, CDM posts several different types of events. You can display detailed information about alarms and events in the Event Browser window.

See Appendix A, "Viewing Alarms and Events," for more detailed information about viewing alarms and events.

Getting Started Using CDM

This chapter describes the tasks you must perform to begin working with CDM. To manage Cisco DSLAMs on the network, you should be familiar with the Cisco EMF and CDM GUIs. This chapter briefly describes the Cisco EMF portion of the software, but mainly describes the CDM user interface.

This chapter includes the following sections:

Note See Appendix D, "Finding Tasks and Related Windows" for a list of all tasks related to setting up and managing DSLAMs through the CDM GUI, the related windows, and links to the associated procedures.

Tasks for Getting Started

The following tasks are required to get started with CDM and the documents in which to find the instructions.

	Task	Cisco Document Reference
Step 1	Install Cisco EMF before you install CDM.	*Cisco Element Management Framework User Guide*
Step 2	Start Cisco EMF before you install CDM. Do not begin a user session at this time.	*Cisco Element Management Framework User Guide*
Step 3	Install CDM.	*Installation Notes for the Cisco DSL Manager NI-1 and NI-2, Release 3.4*
Step 4	Start a Cisco EMF user session. When you start a Cisco EMF user session, CDM starts up automatically.	*Cisco Element Management Framework User Guide*
Step 5	Deploy a site from which Cisco DSLAMs, and its objects, are to be managed.	*Cisco Element Management Framework User Guide*
Step 6	Deploy chassis and chassis objects through a combination of Cisco EMF and CDM functions.	*Cisco Element Management Framework User Guide* Cisco DSL Manager NI-2 User Guide
Step 7	If you have used autodiscovery for a chassis, set passwords. After you manually deploy a chassis, and before you can commission it, you must enter the Cisco IOS command line security password information and enable the password.	See the "Manually Deploying a Cisco DSLAM Chassis" section on page 2-13. Also see the "Specifying Chassis Information and Setting the Cisco IOS Passwords" section on page 2-28.
Step 8	Commission a DSLAM chassis so that the software can actively manage the chassis and the cards within the chassis.	See the "Commissioning a Cisco DSLAM Chassis" section on page 2-31.
Step 9	Set up subscribers; use default xDSL profiles or create new profiles. Set up subscriber connections and upload QoS profiles.	See Chapter 3, "Creating and Applying xDSL Profiles," and Chapter 4, "Creating Connections and ATM QoS Profiles."
Step 10	Manage Cisco DSLAM objects—View alarms, status, and current and historical data, and manage inventory of network objects.	See Chapter 7, "Viewing System and Object Status,"Chapter 8, "Viewing Performance Data," Chapter 9, "Viewing Inventory and Summary Information," and Appendix A, "Viewing Alarms and Events."

Information about Installing Cisco EMF and CDM

Refer to the *Installation Notes for the Cisco DSL Manager NI-1 and NI-2, Release 3.4* for instructions on installing CDM. Refer to the *Cisco Element Management Framework Installation and Administration Guide, Release 3.2* document for instructions on installing Cisco EMF.

Starting a Cisco EMF User Session

Each active Cisco EMF session requires a single Cisco EMF license. To start a Cisco EMF session, follow these steps.

Note Cisco EMF should already be running. If, upon starting, you receive a message that Cisco EMF is not running, contact your system administrator.

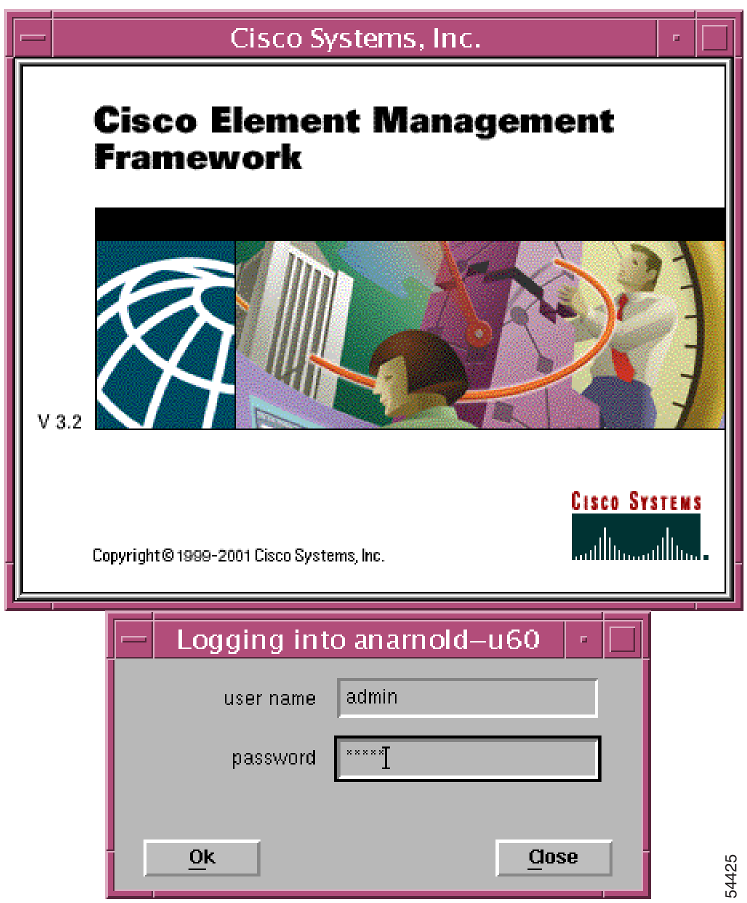
Step 1 At the UNIX prompt, enter the following command:

CEMFROOT/bin/cemf session

Replace **CEMFROOT** with the root directory location in which Cisco EMF Version 3.x is installed. For example, **/opt/cemf3**.

The Login window opens. (See Figure 2-1.)

Figure 2-1 Login Window



Step 2 Enter your user name and password.

When you initially log in to Cisco EMF/CDM, enter **admin** (all lowercase) in the user name and password fields.

Note After you use the initial password to log in, your system or network administrator can use the Cisco EMF access manager to create user groups and new passwords. see the chapter about user access control in the *Cisco Element Management Framework User Guide* for more information.

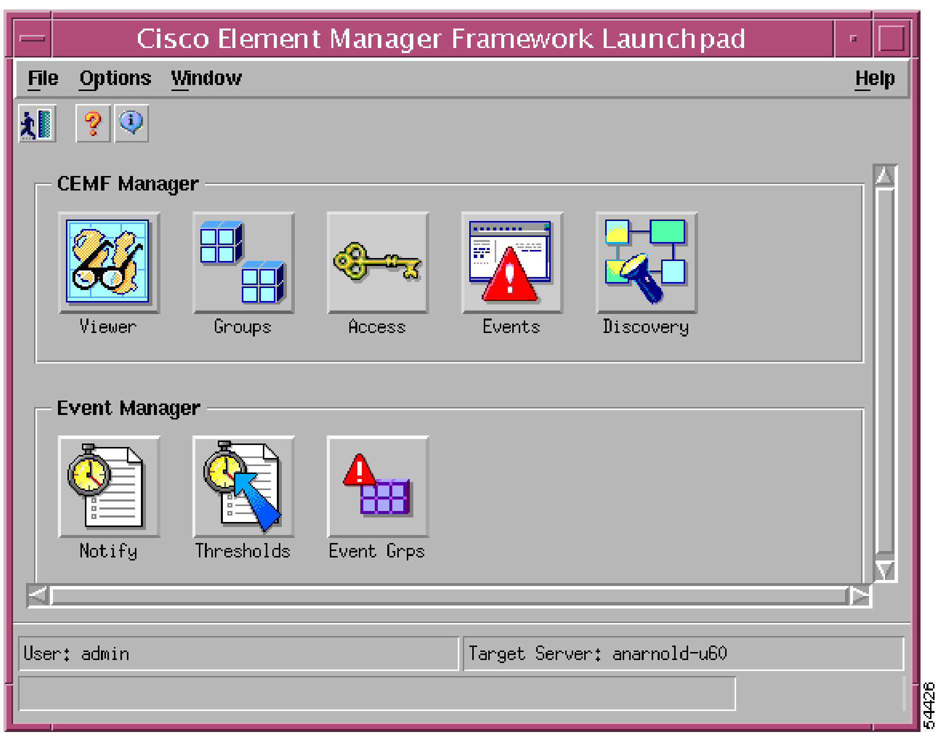
Step 3 Click **OK** to proceed.

If you enter an unknown user name or password, CDM displays an error message. To continue, click **OK**, and then enter a valid user name and password.

Note You are allowed three attempts to enter a valid user name and password. If you do not enter a valid user name and password after three attempts, the session does not start and the Login window closes.

When you enter a valid user name and password, the session starts and the Cisco EMF Launchpad window opens. (See Figure 2-2.)

Figure 2-2 Cisco Element Manager Framework Launchpad Window



Note For more information about using the Cisco EMF Launchpad window, see the "Using the Cisco EMF Launchpad" section on page 1-8.

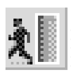
Ending a Cisco EMF User Session

To end or exit from a Cisco EMF user session, follow these steps:

Step 1 Choose one of the following methods to quit the session:

- Choose **Quit** from the File menu.
- Press **Ctrl + Q**.
- Click the **Close** icon from the Toolbar. (See Figure 2-3.)

Figure 2-3 Close Icon



39003

A dialog box opens that asks whether you wish to quit the Cisco EMF Manager System.

Step 2 Click **Yes** to quit the session.

All active applications close and the session terminates.

Using CDM

This section includes the following topics:

To start a CDM session, you must first start Cisco EMF by using the **cemf start** command. You use the **cemf session** command to launch the Map Viewer window, from which you can perform all CDM tasks. When you start Cisco EMF, CDM automatically starts too. The first step to managing a network with CDM is to deploy the DSLAM chassis and then commission it, which initiates autodiscovery of the DSLAM NI-2 card, line cards, and any preprovisioned settings and *x*DSL profiles.

Deploying Objects

This section includes the following topics:

- Manually Deploying Objects, page 2-6
- Autodiscovery Process, page 2-6
- Preprovisioning Feature, page 2-6

Using CDM, you can deploy objects manually or let the software automatically deploy Cisco equipment on the network. You can also deploy objects before they are physically installed in a Cisco DSLAM in the field. CDM detects the presence of previously deployed network equipment as soon as that equipment becomes operational.

Manually Deploying Objects

If you have only a few objects to deploy, use manual deployment. When you choose the Deploy option, you open the Deployment Wizard window, which guides you through the deployment process.

Autodiscovery Process

Autodiscovery automatically discovers existing networks, saving time and effort that you might otherwise spend manually discovering networks. Autodiscovery interrogates the network for IP and SNMP devices, then creates an object for each new device it discovers. Autodiscovery is an efficient way to discover Cisco DSLAMs that are already installed. See the "The Autodiscovery Process" section on page 1-7 for a more detailed description of autodiscovery.

Preprovisioning Feature

Preprovisioning is a type of deployment. The difference between deployment and preprovisioning is that you preprovision an object *before* the hardware is actually present; you deploy an object when the hardware *is* present. Preprovisioning allows you to deploy cards within a chassis before they are physically installed in the hardware.

You can also configure a preprovisioned card. For example, if you know a 4DMT card is to be installed in a chassis, you can deploy and preprovision the 4DMT card in a selected chassis and perform all relevant 4DMT card configurations. When the 4DMT card becomes physically available, CDM accepts the configuration you have already performed. The system does not monitor preprovisioned objects, which means that alarm, status, and performance information are not available for preprovisioned hardware.

When the 4DMT card is physically inserted in a card slot in the chassis, subscribers and line card configuration are immediately loaded into that line card. The software automatically detects the existence of the cards and moves the cards into the Normal state. You can then monitor alarm, status, and performance information on the card.

Note You can deploy preprovisioned line cards only if the related Cisco DSLAM chassis and NI-2 card are in a Normal or Decommissioned state.

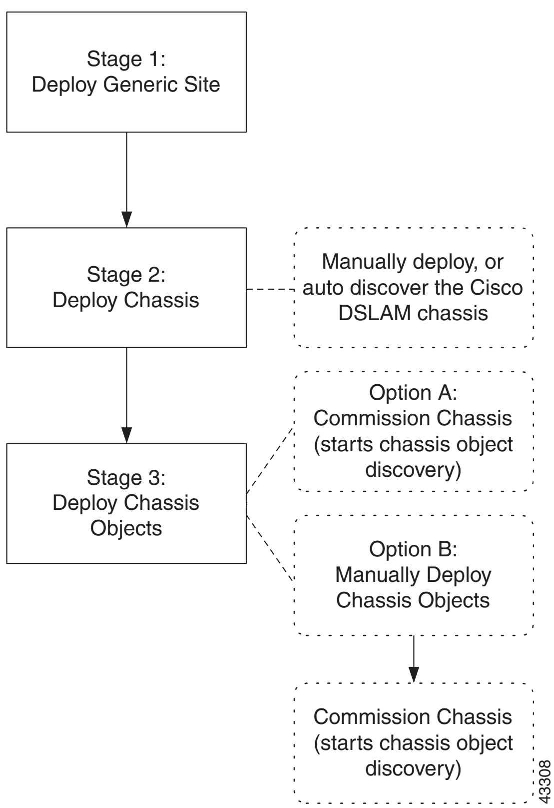
Deployment Process

To configure a Cisco DSLAM that the software can manage, you must first deploy the generic site in which you want the Cisco DSLAM located. (A generic object is a nontechnology-specific object.) You can deploy the site by opening the Deployment Wizard template. After you successfully deploy the generic site, you can begin deploying the chassis and chassis objects.

To deploy a manageable Cisco DSLAM, follow these guidelines (see Figure 2-4 for a visual guide):

1. Deploy generic site—Deploy the generic site using the Deployment Wizard template. Refer to the *Cisco Element Management Framework User Guide* for information on deploying a site.
2. Deploy DSLAM chassis—Deploy the Cisco DSLAM chassis manually or use the Autodiscovery feature. (See the "The Autodiscovery Process" section on page 1-7.)
3. Deploy DSLAM chassis objects using one of the following methods:
   - Commissioning the deployed chassis, and letting CDM automatically discover chassis objects (NI-2 cards and line cards).
   - Manually deploying chassis objects, and then commissioning the chassis. The system then discovers the chassis objects.

Figure 2-4 Deployment Process



Deploying a Generic Site

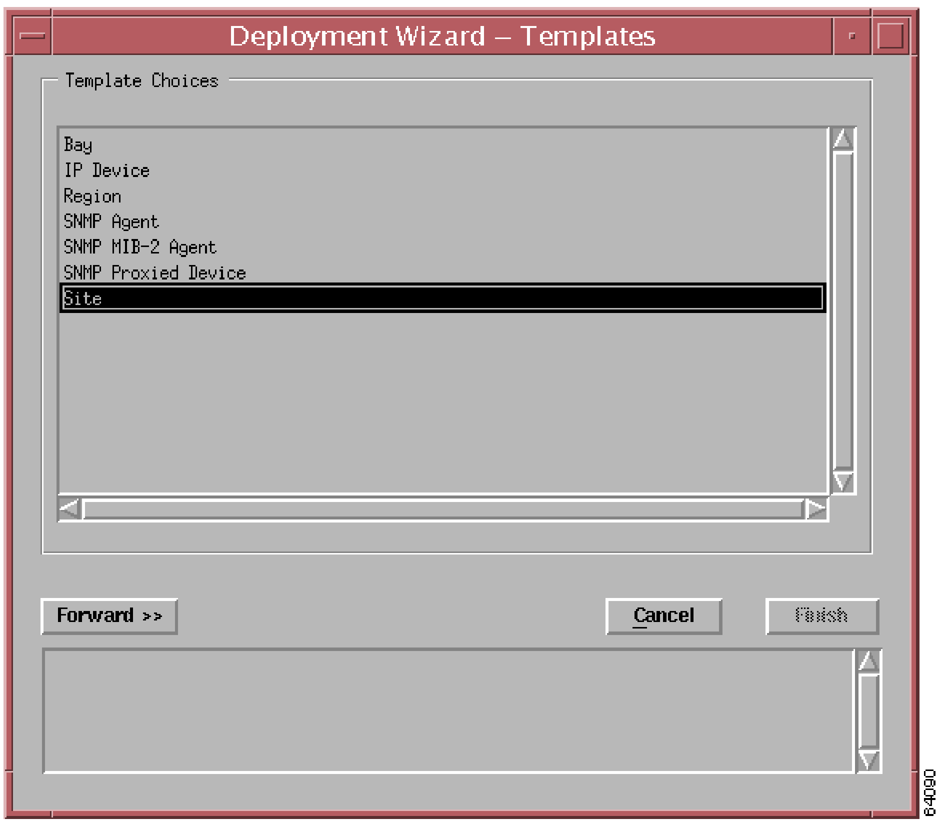
Before you deploy a Cisco DSLAM chassis, you must deploy one or more generic sites under which you can then deploy DSLAMs. Complete the following steps to deploy a generic site:

Step 1 From the left side of the Map Viewer window, right-click the Physical map hierarchy view icon.

Step 2 Choose **Deployment > Deploy Generic Objects** from the object menu.

The Deployment Wizard—Templates window opens. (See Figure 2-5.)

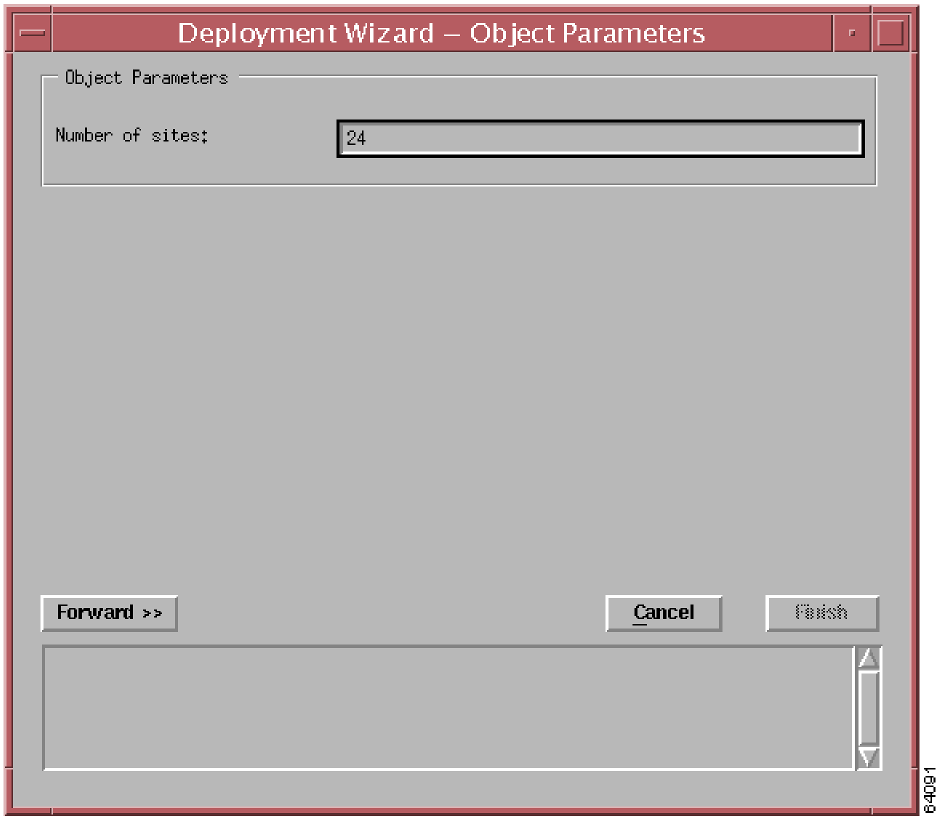
Figure 2-5 Deployment Wizard—Templates Window



Step 3 Click **Site**, then click **Forward**.

The Deployment Wizard—Object Parameters Window opens. (See Figure 2-6.)

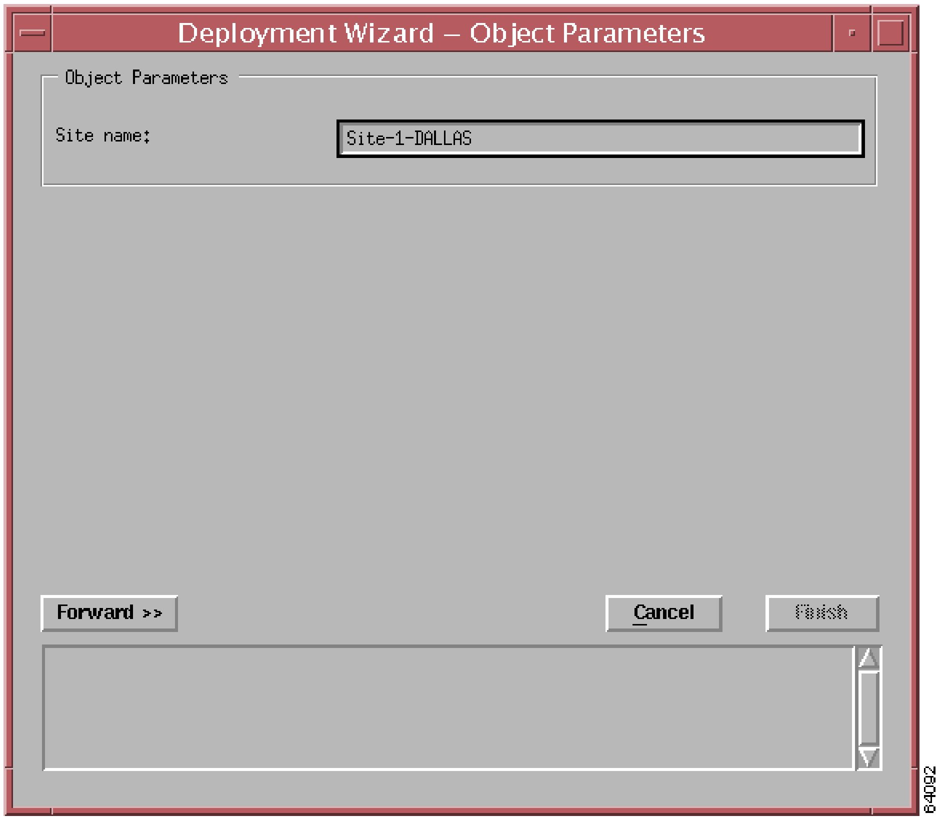
Figure 2-6 Deployment Wizard —Object Parameters Window



Step 4 Enter the number of sites that you want to deploy in the Number of Sites field, and then click **Forward**.

The next Deployment Wizard—Object Parameters window opens. (See Figure 2-7.)

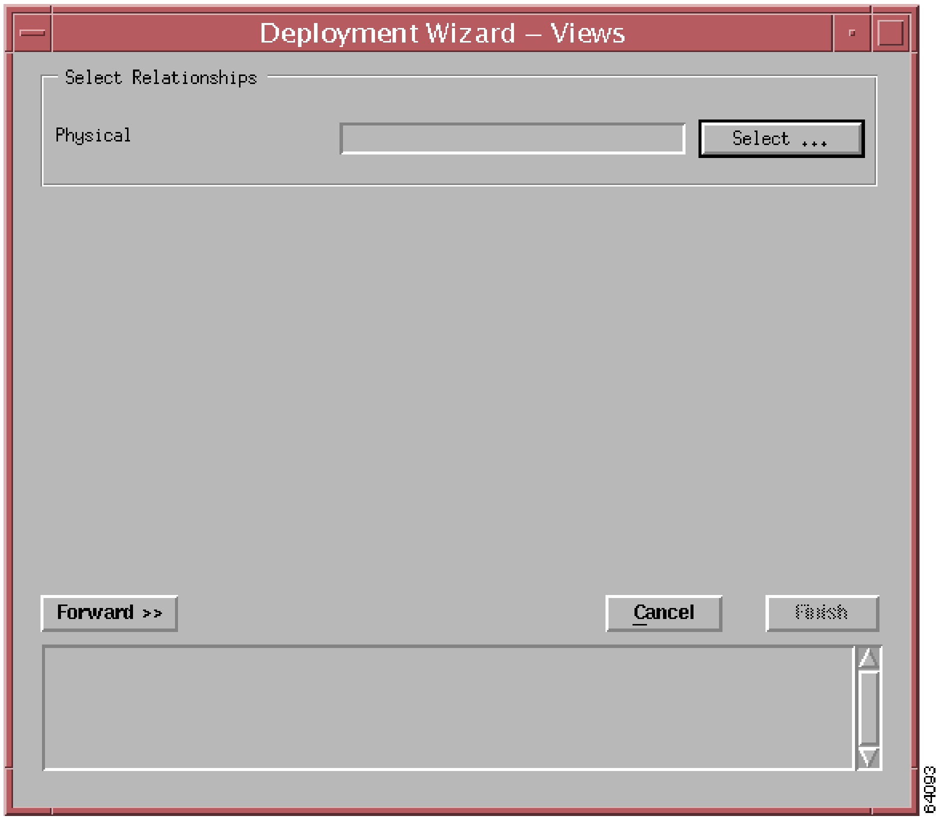
Figure 2-7 Deployment Wizard—Object Parameters Window



Step 5 Enter the name of the site in the Site Name Field, then click **Forward**.

The Deployment Wizard—Views window opens. (See Figure 2-8.)

Figure 2-8 Deployment Wizard—Views Window



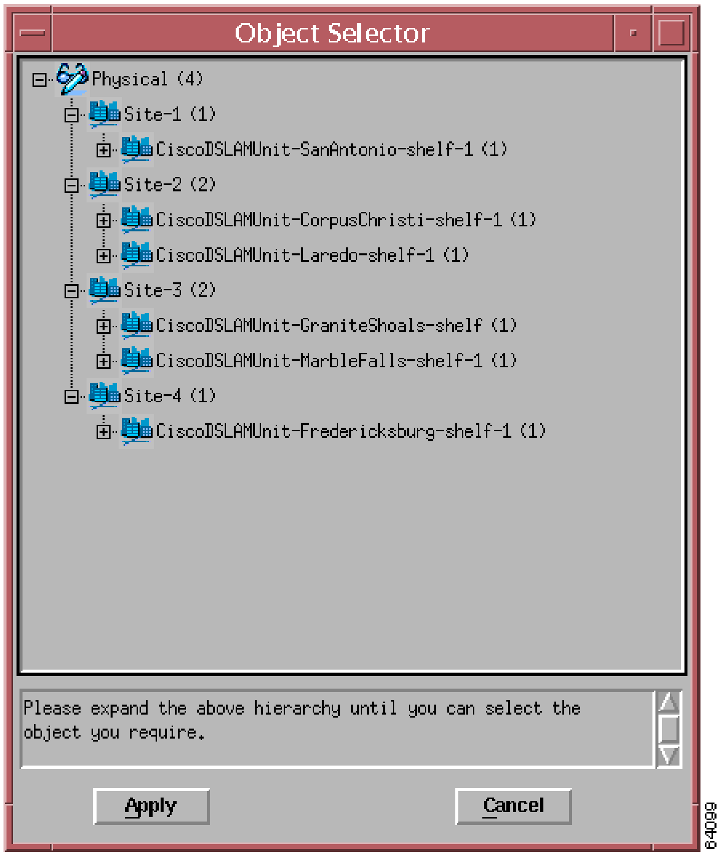
Step 6 Repeat Step 5 for each site that you want to deploy.

For example, if you entered 24 in the Number of Sites field (in Step 4), CDM prompts you to enter the name for each of the 24 sites.

Step 7 Click **Select** next to the Physical field.

The Object Selector window opens. (See Figure 2-9.)

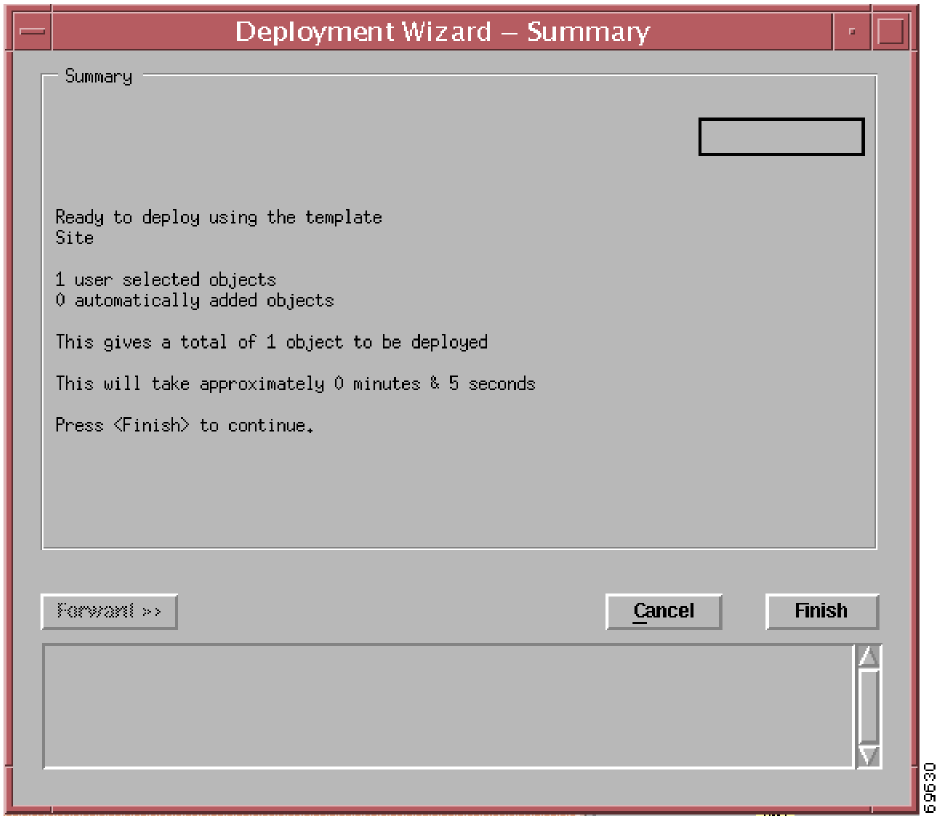
Figure 2-9 Object Selector Dialog Box



Step 8 Click **Physical**, and then **Apply** to apply this site to the Physical view.

The Deployment Wizard—Summary window opens. (See Figure 2-10.)

Figure 2-10 Deployment Wizard—Summary Window



Step 9 Click **Finish** to deploy the generic site or sites.

Step 10 Repeat Step 5 through Step 9 for each site. For example, if you entered 24 in the Number of Sites field (in Step 4), CDM prompts you to enter the name for each of the 24 sites.

Step 11 Verify that the sites you have deployed display on the left side of the Map Viewer window.

Manually Deploying a Cisco DSLAM Chassis

You can manually deploy a Cisco DSLAM chassis from the Map Viewer window. To access the Map Viewer, click the **Viewer** icon in the Launchpad. When you deploy a Cisco DSLAM chassis, you are configuring the chassis and SNMP parameters for the chassis. You manually deploy a DSLAM chassis through the Deployment Wizard window.

Note Before you deploy a DSLAM chassis, you must deploy a site (see the "Deploying a Generic Site" section on page 2-8 for these instructions).

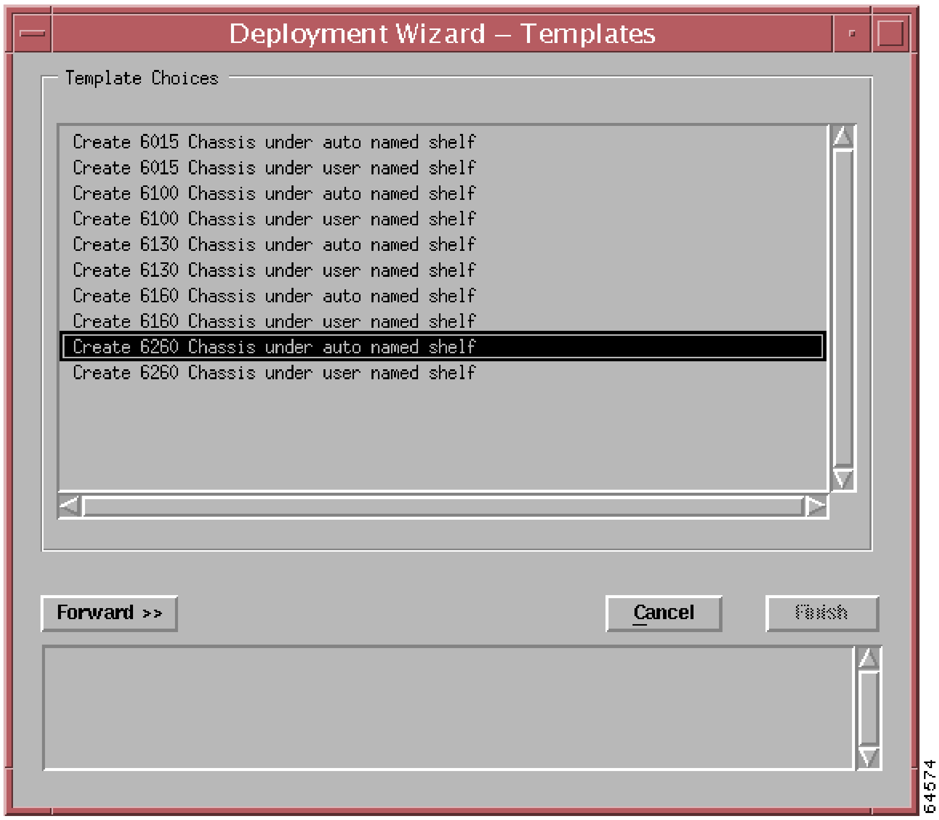
To manually deploy a Cisco DSLAM chassis under a site, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the CDM Manager view, right-click the site to access the object menu.

Step 2 Choose **Deployment > Deploy Cisco DSLAM**.

The Deployment Wizard—Templates window open. (See Figure 2-11.)

Figure 2-11 Deployment Wizard—Templates Window

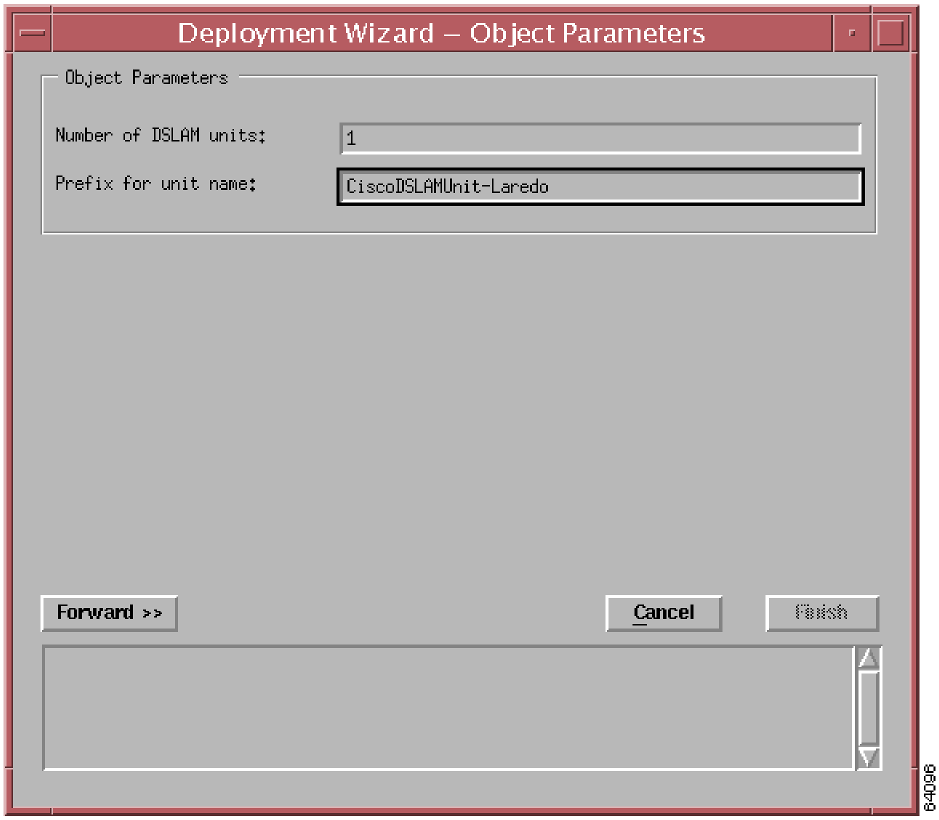


Step 3 Click **Create <DSLAM type> Chassis under auto named shelf** or **Create <DSLAM type> Chassis under user named shelf**, and then click **Forward**.

Tip You can have CDM name the DSLAM chassis, or you can create a name for the chassis.

The Deployment Wizard—Object Parameters window opens. (See Figure 2-12.)

Figure 2-12 Deployment Wizard—Object Parameters Window



Step 4 Enter the appropriate number of DSLAMs in the DSLAM units field.

Step 5 Enter the name for the DSLAM units in the Prefix for unit name field.

Step 6 Click **Forward** to proceed.

Note Cisco recommends that you deploy one chassis at a time.

Note If you choose to deploy a chassis under a user-named shelf, the Number of DSLAM units and Prefix for unit name fields display in two separate Deployment Wizard—Object Parameters windows.

Step 7 In the Prefix for unit name field, accept the default prefix that CDM generates, or enter a unique prefix for the unit name.

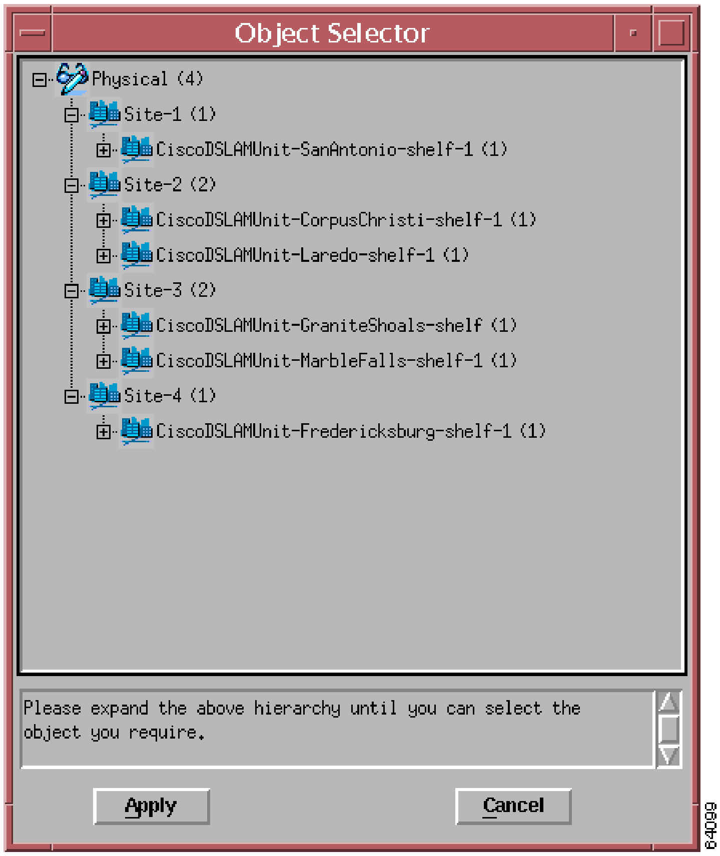
The value that you enter in the Prefix for unit name field carries over to the Chassis Name field to minimize duplicate data entry. You can use the default value, change the value, or delete the default value to exclude it from part of the Chassis Name field.

Step 8 Click **Forward** to continue.

Step 9 Click **Select** next to the Physical field to select the Physical site under which you want to deploy this DSLAM.

The Object Selector dialog box opens. (See Figure 2-13.)

Figure 2-13 Object Selector Dialog Box



Step 10 Click the **+** next to Physical to display the sites that are deployed.

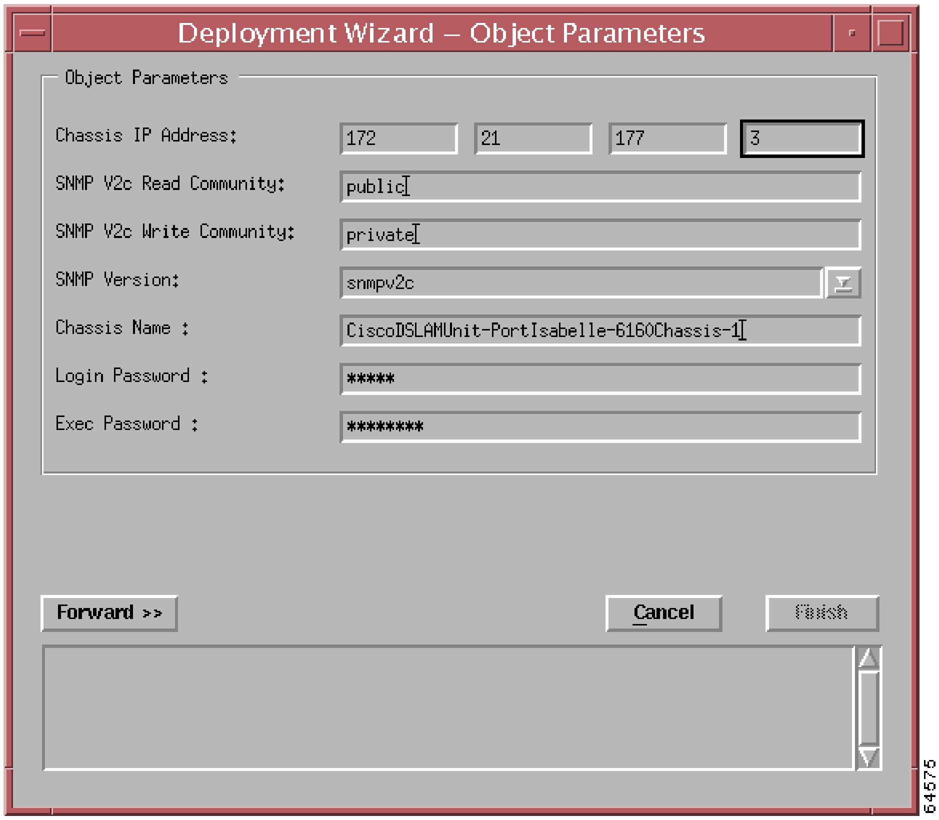
Step 11 Click the site under which you want to deploy the DSLAM chassis.

The Deployment Wizard—Views window reopens and displays the Site that you selected in the Object Selector dialog box next to the Physical and Component Managed fields.

Step 12 Click **Forward** to continue.

The next Deployment Wizard—Object Parameters window opens. (See Figure 2-14.)

Figure 2-14 Deployment Wizard—Object Parameters Window



Step 13 Enter the appropriate information in the fields in this window, as follows:

a. In the Chassis IP Address field, enter the valid IP address for the chassis you are deploying; the maximum alphanumeric limit is 15 characters.

Contact your system administrator if you do not know the IP address.

b. In the SNMP V2c Read Community field, enter the name for the read-only relationship; the name that you enter must match the SNMP community read string on the Cisco DSLAM.

The default entry might not match the Cisco DSLAM privileges; be sure to enter a name that matches the SNMP community read string.

c. In the SNMP V2c Write Community field, enter the name for the read-write relationship; the name you enter here must match the SNMP write community string on the Cisco DSLAM.

You must replace the default entry; it might not match the Cisco DSLAM privileges.

d. In the SNMP Version field, enter the version of SNMP that is running on the equipment in the Chassis IP Address field from the following choices:

- snmpv1
- snmpv2c
- snmpv3 (not supported)

e. In the Chassis Name field, use the default chassis name (that CMD generates as a result of your entry in the Prefix for Unit Name field) or enter a unique name for the chassis you are deploying.

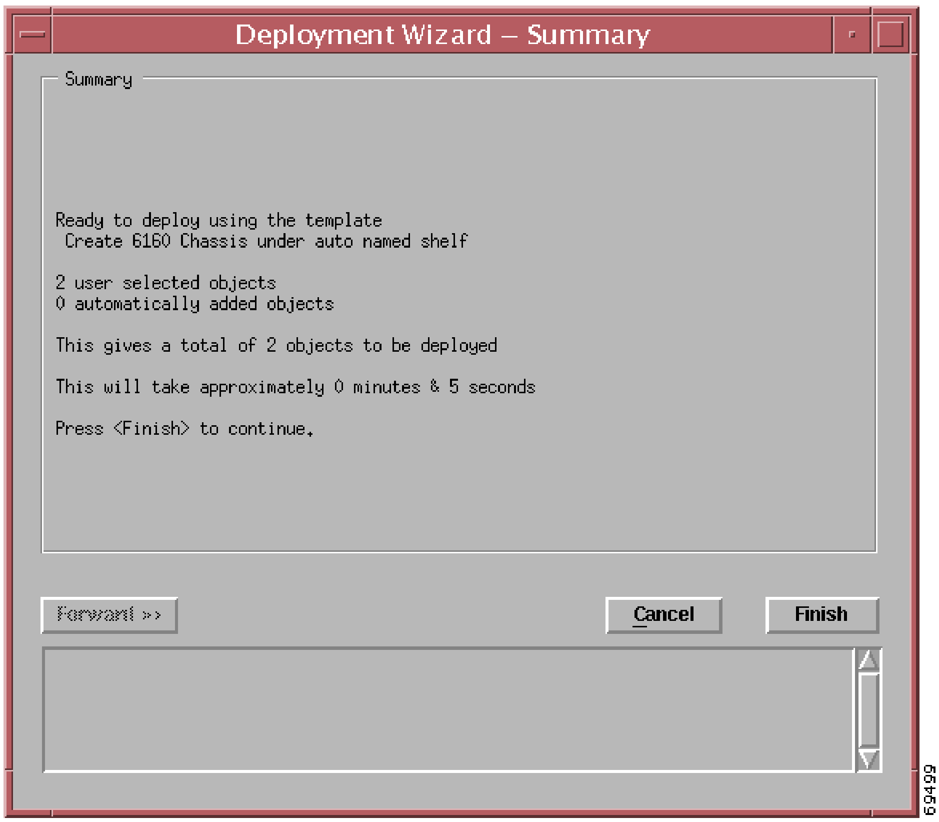
f. In the Login Password field, enter the login password for this DSLAM.

g. In the Exec Password field, enter the executive password for this DSLAM; this password should match the IOS privileged password for the IOS that is running on the DSLAM.

Step 14 Click **Forward** to complete the deployment process.

The Deployment Wizard Summary window opens and informs you that CDM is ready to deploy the DSLAM chassis. (See Figure 2-15.)

Figure 2-15 Deployment Wizard Summary Window



The Deployment Wizard Summary window prompts you to commit or reject the deployment. When you deploy a chassis, a shelf object is also created (thus deploying two objects), as shown in the Deployment Wizard Summary window (see Figure 2-15).

Step 15 To commit the deployment, click **Finish**; to reject the deployment, click **Cancel**.

If the deployment is successful, the object appears in the chassis view. If the deployment is unsuccessful, the Deployment Wizard—Summary window informs you that the deployment failed.

If the DSLAM that you deployed is populated and ready to be managed on the network, you need to commission it next. See the “Commissioning the DSLAM and other Network Elements” section on page 2-31 for instructions on how to commission the DSLAM and begin managing its network elements.

If after you have commissioned a DSLAM, you need to change or replace an NI card or a line card, you can first preprovision the card, and then manually deploy the card. The following sections provide instructions on manually deploying cards on a DSLAM.

Manually Deploying a Line Card

This section includes the following topics:

- Deployment Wizard—Object Parameter Field Definitions for the 8xDMT Card, page 2-24
- Deployment Wizard—Object Parameter Field Definitions for the 4xSDSL Card, page 2-25
- Deployment Wizard—Object Parameter Field Definitions for the 4xflexi Card, page 2-26

Table 2-1 lists the types of line cards that you can deploy on each DSLAM through the CDM interface.

Table 2-1 Line Card Deployment

	DSLAMs Supported				
Line Card	**Cisco 6015**	**Cisco 6100**	**Cisco 6130**	**Cisco 6160**	**Cisco 6260**
8xDMT	yes	no	no	yes	yes
8xDMTC	yes	no	no	yes	yes
8xG.SHDSL	yes	no	no	yes	yes
FlexiCAP	yes	yes	yes	yes	no
FlexiDMT	yes	yes	yes	yes	yes
DMT	no	yes	yes	yes	no
DMT over ISDN	yes	no	no	no	yes
SDSL	no	no	yes	yes	yes

When you deploy a line card, you are configuring the parameters for the card. This section describes how you deploy a line card, and it provides the parameters (field definitions) for each of the basic types of line cards supported by the various DSLAM chassis. These instructions pertain to a DMT line card, but they can apply to any type of line card that is supported on the Cisco DSLAMs.

Note Be aware of the intermixing rules and compatibility issues for Cisco DSLAMs. Refer to the following Cisco publications: *Cisco DSLAM Compatibility Notes*, *Cisco 6100 with NI-2 Hardware Installation Guide*, *Cisco 6130 with NI-2 Hardware Installation Guide*, *Cisco 6015 Hardware Installation Guide*, *Cisco 6160 Hardware Installation Guide*, and *Cisco 6260 Hardware Installation Guide*. These documents provide the most up-to-date information. You can navigate to each of these publications from the following URL: http://www.cisco.com/univercd/cc/td/doc/product/dsl_prod/index.htm.

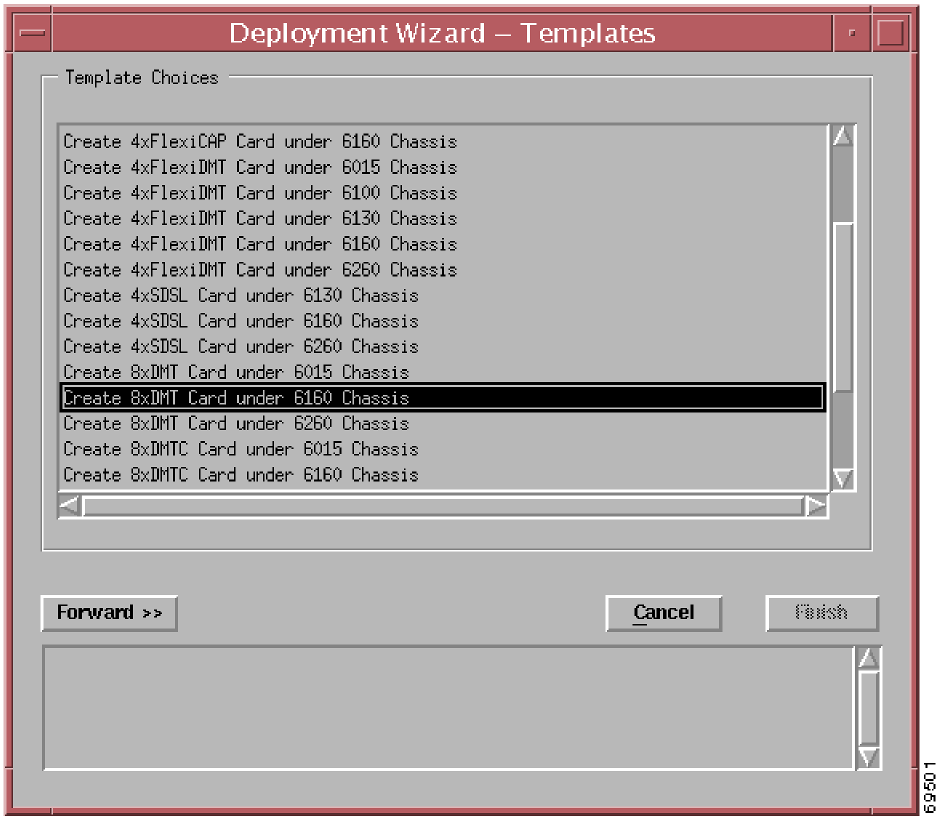
To manually deploy a line card in a chassis, complete the following steps:

Step 1 In the Map Viewer window, right-click the chassis in which you want to deploy a line card.

Step 2 Choose **Deployment > Deploy Cisco DSLAM** from the object menu.

The Deployment Wizard—Templates window opens. (See Figure 2-16.)

Figure 2-16 Deployment Wizard—Templates Window



Step 3 Click **Create [type of card] Card under <DSLAM type> Chassis**, then click **Forward**.

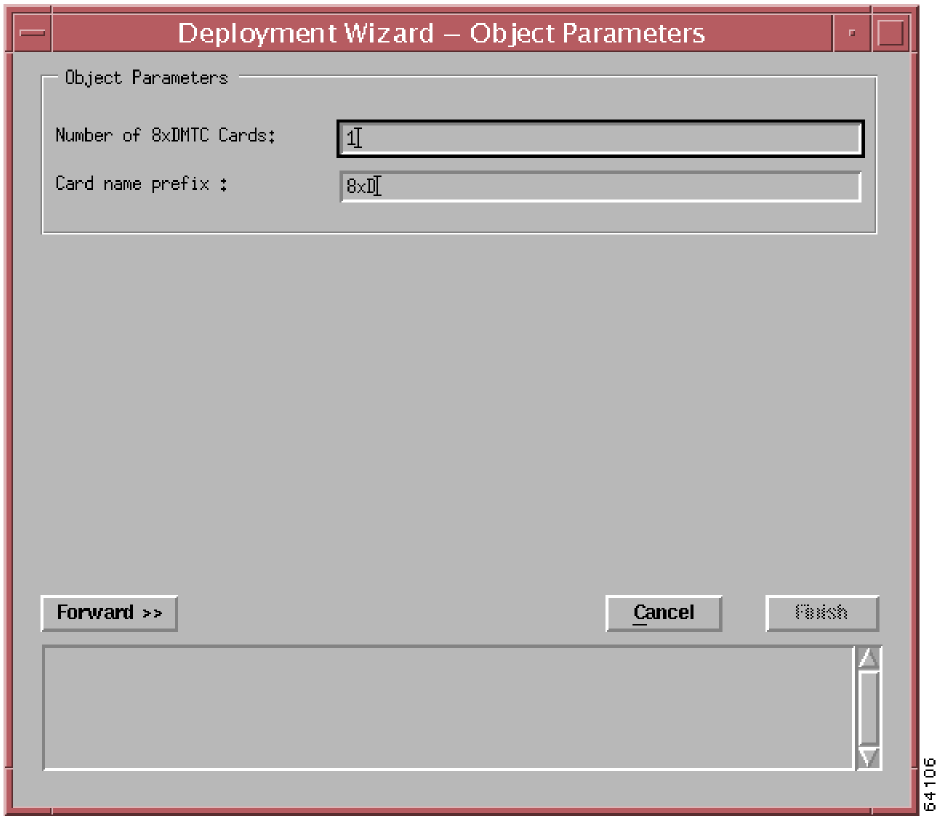
The first of two or more Deployment Wizard—Object Parameters windows opens.

The instructions for entering information in the Deployment Wizard—Object Parameters windows that follow are generic. Definitions for the fields that are specific to the type of line card are described in the following tables:

- Table 2-2 on page 2-24—Deployment Wizard—Object Parameters Field Definitions for the 8xDMT Card—The fields in these tables apply to deploying any type of DMT line card.
- Table 2-3 on page 2-25—Deployment Wizard—Object Parameters Field Definitions for the 4xSDSL Card—The fields in these tables apply to deploying any type of SDSL or G.SHDSL line card.
- Table 2-4 on page 2-27—Deployment Wizard—Object Parameters Field Definitions for the 4xflexi Card—The fields in these tables apply to the deploying of any type of Flexi line card.

The Deployment Wizard—Object Parameters window opens. (See Figure 2-17.)

Figure 2-17 Deployment Wizard—Object Parameters Window



Step 4 Enter the appropriate information in the Deployment Wizard—Object Parameters window, as follows:

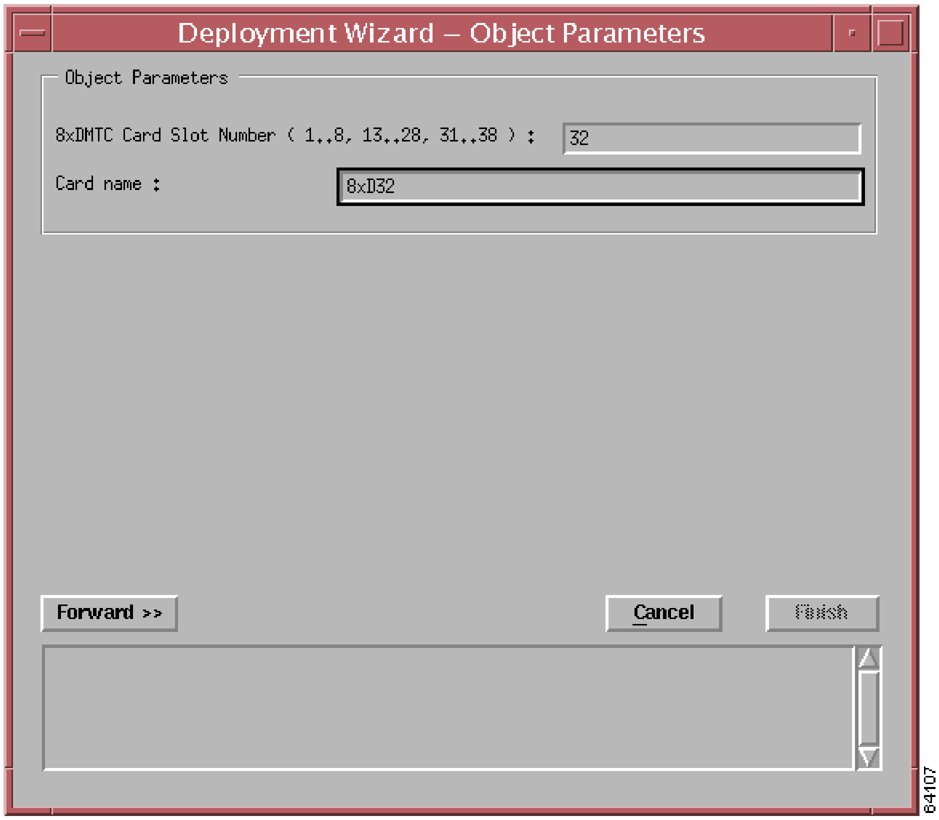
a. In the Number of [type of card] Cards field, enter the number of line cards that you want to deploy for this chassis; for the 6100, 6130, and 6160, the maximum number is 32.For the 6260, the maximum number is 30, and for the 6015, the maximum number is 6 slots.

b. In the Card name prefix field, accept the default prefix, or enter a unique prefix for the card name.

The value that you enter in the Card name prefix field carries over to the Card Name field to minimize duplicate data entry. You can use the default value, change the value, or delete the default value to exclude it from part of the Card Name field.

The next Deployment Wizard—Object Parameters window opens. (See Figure 2-18.)

Figure 2-18 Deployment Wizard—Object Parameters Window



Step 5 Enter the appropriate information in the Deployment Wizard—Object Parameters window, as follows:

a. In the [type of card] Card Slot Number field, enter the slot number in which the line card will be installed in the Cisco DSLAM chassis.

Valid values for each type of DSLAM are as follows:

- For the 6100—1 to 8, 13 to 28, and 31 to 38 (slots 10 and 11 are reserved for NI-2 cards; slots 9, 29, and 30 are reserved for future development; and slot 12 is reserved for a jumper card).
- For the 6130—1 to 8, 13 to 28, and 31 to 38 (slots 10 and 11 are reserved for NI-2 cards with slot 11 available to support NI-2 card redundancy; slots 9, 12, 29, and 30 are reserved for future development).
- For the 6160—1 to 9 and 12 to 34 (slots 10 and 11 are reserved for the NI-2 cards).
- For the 6260—1 to 9 and 12 to 32 (slots 10 and 11 are reserved for the NI-2 cards).
- For the 6015—1 to 6

If you chose to deploy more than one card in the Number of [type of card] Cards field, this field (and the Card Name field) remain visible until you enter data for each of the [type of card] cards you are deploying. The Deployment Wizard Summary window appears only after you assign a slot number and card name for each card you are deploying.

b. In the Card Name field, accept the default card name (that is generated as a result of your entry in the Card Name Prefix field) or enter a unique name for the line card.

An example of a unique card name is DMT6*XXX*slot2 (where DMT is the card name, 6*XXX* is the chassis in which the card is installed, and slot2 is the physical location of the card in the chassis). If you are deploying multiple DMT cards for this chassis, CDM retains the card name that you entered for the first DMT card and adds a digit to the end of the card name, for each subsequent card, to indicate which card you are currently configuring.

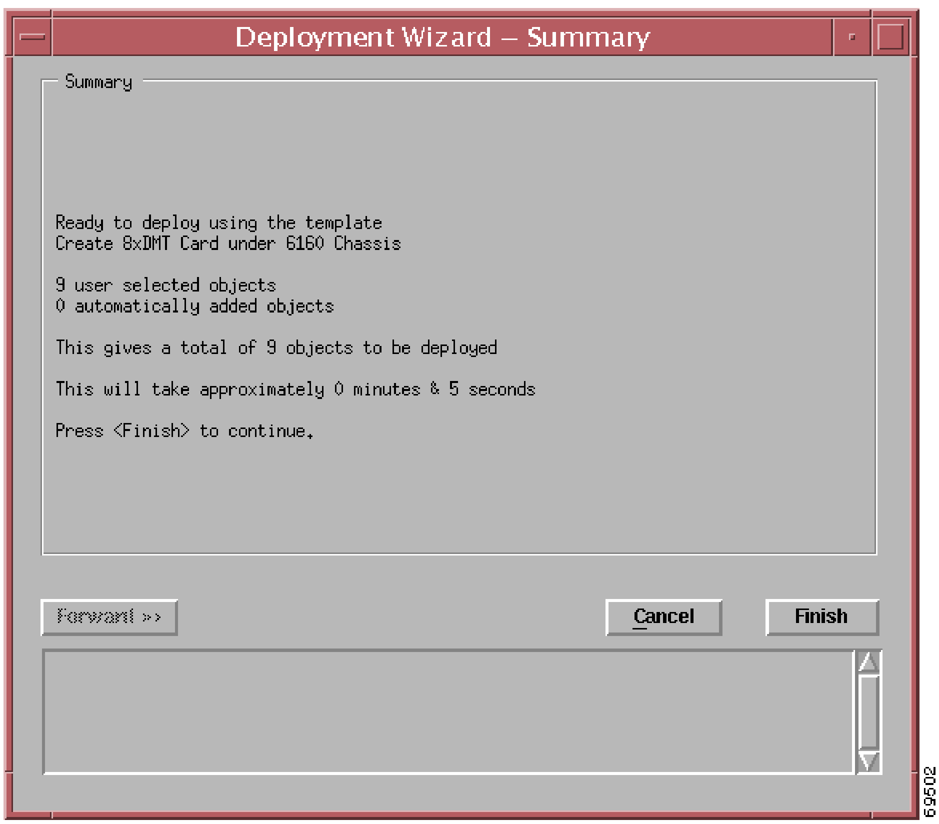
Step 6 Click **Forward** to continue.

Note If you are deploying more than one line card, the software automatically increments the values in the fields in the second Deployment Wizard—Object Parameters window to indicate the card you are currently configuring. You can accept or overwrite the default values.

For example, if the Card Name value for the first line card is DMT1, the value in the Card Name field for the second line card displays as DMT2.

After you configure the parameters in the Deployment Wizard—Object Parameters windows, the Deployment Wizard Summary window opens. (See Figure 2-19.)

Figure 2-19 Deployment Wizard Summary Window—Line Card



The Deployment Summary window displays the number of objects CDM is ready to deploy. In this example, CDM is deploying an 8xDMT line card, which includes 8 ports and a line card—a total of 9 objects to be deployed.

Step 7 To commit the deployment, click **Finish**. To reject the deployment, click **Cancel**.

If the deployment is successful, the object appears in the chassis view. If the deployment is not successful, a feedback window informs you that the deployment failed.

Note When you deploy a line card, the interfaces (that represent the ports on a line card) are automatically deployed as well. Therefore, the number of ports plus the interface are deployed for a line card.

Deployment Wizard—Object Parameter Field Definitions for the 8xDMT Card

Table 2-2 describes the fields that are located in the Deployment Wizard—Object Parameters (8xDMT card) window.

Table 2-2 Deployment Wizard—Object Parameters Field Definitions for the 8xDMT Card

Field	Description
Number of DMT Cards	Enter the number of DMT cards you want to deploy for the chassis that you selected from the Deployment Wizard—Templates window using the following guidelines: • The maximum number for the 6160 is 32. • The maximum number for the 6260 is 30 • The maximum number for the 6015 is 6.
Card Name Prefix	Accept the default prefix that CDM generates, or enter a unique prefix for the card name. The value that you enter in the Card Name Prefix field carries over to the Card Name field to minimize duplicate data entry. You can use the default value, change the value, or delete the default value to exclude it from part of the Card Name field.

Table 2-2 Deployment Wizard—Object Parameters Field Definitions for the 8xDMT Card (continued)

Field	Description
DMT Card Slot Number	Enter the slot number in which you will install the DMT card in the Cisco DSLAM using the following guidelines. • Valid values for the 6160 are 1 to 9 and 12 to 34. (Slots 10 and 11 are reserved for NI-2 cards.) • Valid values for the 6260 are 1 to 9 and 12 to 32. (Slots 10 and 11 are reserved for the NI-2 cards.)Valid values for the 6015 are 1 to 6. If you chose to deploy more than one card in the Number of DMT Cards field, this field and the Card Name field remain visible until you enter data for each of the DMT cards you are deploying. The Deployment Summary window opens only after you assign a slot number and card name for each card you are deploying.
Card Name	Use the default card name that CDM generates as a result of your entry in the Card Name Prefix field, or enter a unique name for the DMT card. An example of a unique card name is DMT6160slot2, where DMT is the card name, 6160 is the chassis in which the card is installed, and slot2 is the physical location of the card in the chassis. If you are deploying multiple DMT cards for this chassis, CDM retains the card name that you entered for the first DMT card and adds a digit to the end of the card name for each subsequent card. This process indicates which card you are currently configuring.

Deployment Wizard—Object Parameter Field Definitions for the 4xSDSL Card

Table 2-3 describes the fields that are located in the Deployment Wizard—Object Parameters (4xSDSL card) windows.

Table 2-3 Deployment Wizard—Object Parameters Field Definitions for the 4xSDSL Card

Field	Description
Number of SDSL Cards	Enter the number of 4xSDSL cards that you want to deploy for the chassis you selected from the Deployment Wizard—Templates window. The maximum number for the 6130 and 6160 is 32. The maximum number for the 6260 is 30.
Card Name Prefix	Accept the default prefix that CDM generates, or enter a unique prefix for the card name. The value that you enter in the Card Name Prefix field carries over to the Card Name field to minimize duplicate data entry. You can use the default value, change the value, or delete the default value to exclude it from part of the Card Name field.

Table 2-3 Deployment Wizard—Object Parameters Field Definitions for the 4xSDSL Card (continued)

Field	Description
SDSL Card Slot Number	Enter the slot number in which you plan to install the 4xSDSL in the Cisco DSLAM using the following guidelines. • Valid values for the 6130 are 1 to 8, 13 to 28, and 31 to 38 (slots 10 and 11 are reserved for NI-2 cards, and slots 9, 12, 29, and 30 are reserved for future development). • Valid values for the 6160 are 1 to 9 and 12 to 34; slots 10 and 11 are reserved for NI-2 cards. • Valid values for the 6260 are 1 to 9 and 12 to 32 (slots 10 and 11 are reserved for the NI-2 cards). If you chose to deploy more than one card in the Number of SDSL Cards field, this field and the Card Name field remain visible until you enter data for each of the 4xSDSL cards you are deploying. The Deployment Summary window opens only after you assign a slot number and card name for each card you are deploying.
Card Name	Use the default card name that CDM generates as a result of your entry in the Card Name Prefix field, or enter a unique name for the 4xSDSL card. An example of a unique card name is SDSL6160slot2, where SDSL is the card name, 6160 is the chassis in which the card is installed, and slot2 is the physical location of the card in the chassis. If you are deploying multiple 4xSDSL cards for this chassis, CDM retains the card name you entered for the first 4xSDSL card and adds a digit to the end of the card name (for each subsequent card) to indicate which card you are currently configuring.

Deployment Wizard—Object Parameter Field Definitions for the 4xflexi Card

Table 2-4 describes the fields that are located in the Deployment Wizard—Object Parameters (4xflexi card) windows.

Note CDM provides two options for deploying a 4xflexi card—Create Cisco Flexi CAP Line Card and Create Cisco Flexi DMT Line Card. The fields in the Deployment Wizard—Object Parameters windows are the same for the 4xflexi CAP and 4xflexi (DMT), therefore, use the field definitions in this section for both.

Table 2-4 Deployment Wizard—Object Parameters Field Definitions for the 4xflexi Card

Field	Description
Number of Cisco Flexi Cap Card Objects *or* Number of Cisco Flexi DMT Card Objects	Enter the number of 4xflexi cards you want to deploy for the chassis you selected from the Deployment Wizard—Templates window using the following guidelines: • The maximum number for the 6015 is 6. • The maximum number for the 6100, 6130, and 6160 is 32. • The maximum number for the 6260 is 30.
Card Name Prefix	Accept the default prefix that CDM generates, or enter a unique prefix for the card name. The value you enter in the Card Name Prefix field carries over to the Card Name field to minimize duplicate data entry. You can use the default value, change the value, or delete the default value to exclude it from part of the Card Name field.
Flexi CAP Card Slot Number *or* Flexi DMT Card Slot Number	Enter the slot number in which the 4xflexi card will be installed in the Cisco DSLAM chassis using the following guidelines: • Valid values for the 6015 are 1 to 6. • Valid values for the 6100 and 6130 are 1 to 8, 13 to 28, and 31 to 38 (slots 10 and 11 are reserved for NI-2 cards, and slots 9, 12, 29, and 30 are reserved for future development). • Valid values for the 6160 are 1 to 9 and 12 to 34; slots 10 and 11 are reserved for NI-2 cards. • Valid values for the 6260 are 1 to 9 and 12 to 32 (slots 10 and 11 are reserved for the NI-2 cards). If you chose to deploy more than one Flexi card in the Number of Cisco Flexi *XXX* Card Objects field, this field (and the Card Name field) remains visible until you enter data for each of the cards you are deploying. The Deployment Summary window opens only after you assign a slot number and card name for each card you are deploying.
Card Name	Use the default card name (generated as a result of your entry in the Card Name Prefix field) or enter a unique name for the 4xflexi card. An example of a unique card name is FCAP6160slot3 (where FCAP is the card name, 6160 is the chassis in which the card is installed, and slot3 is the physical location of the card in the chassis). If you are deploying multiple flexi cards for this chassis, the system retains the card name you entered for the first flexi card and adds a digit to the end of the card name (for each subsequent card) to indicate which card you are currently configuring.

Specifying Chassis Information and Setting the Cisco IOS Passwords

This section provides instructions to enter the appropriate chassis information in the Management Information window so that you can set the Cisco IOS command line interface (CLI) passwords. This section includes the following topics:

- Setting Chassis Information in the Management Information Window, page 2-28
- Setting the Cisco IOS Command Line Security Password, page 2-30

Some element manager applications use the Cisco IOS CLI. Therefore, after you deploy a chassis, and before you can commission a chassis, you must enter the Cisco IOS command line security password information for the Cisco DSLAM chassis. Setting the IOS CLI security passwords allows CDM to use IOS commands to communicate with the DSLAM through a telnet window that you open from the CDM GUI.

When you manually deploy a DSLAM, you can enter the IOS passwords in the Deployment Wizard window. See the "Manually Deploying a Cisco DSLAM Chassis" section on page 2-13.

You can configure a chassis or its objects only if the system administrator provides you with the appropriate CLI password values. These values are set in the Management Information window, IOS/Command Line Security tab.

Note The system administrator or network manager should be responsible for changing the Cisco IOS CLI security passwords; general users should not change these passwords.

Setting Chassis Information in the Management Information Window

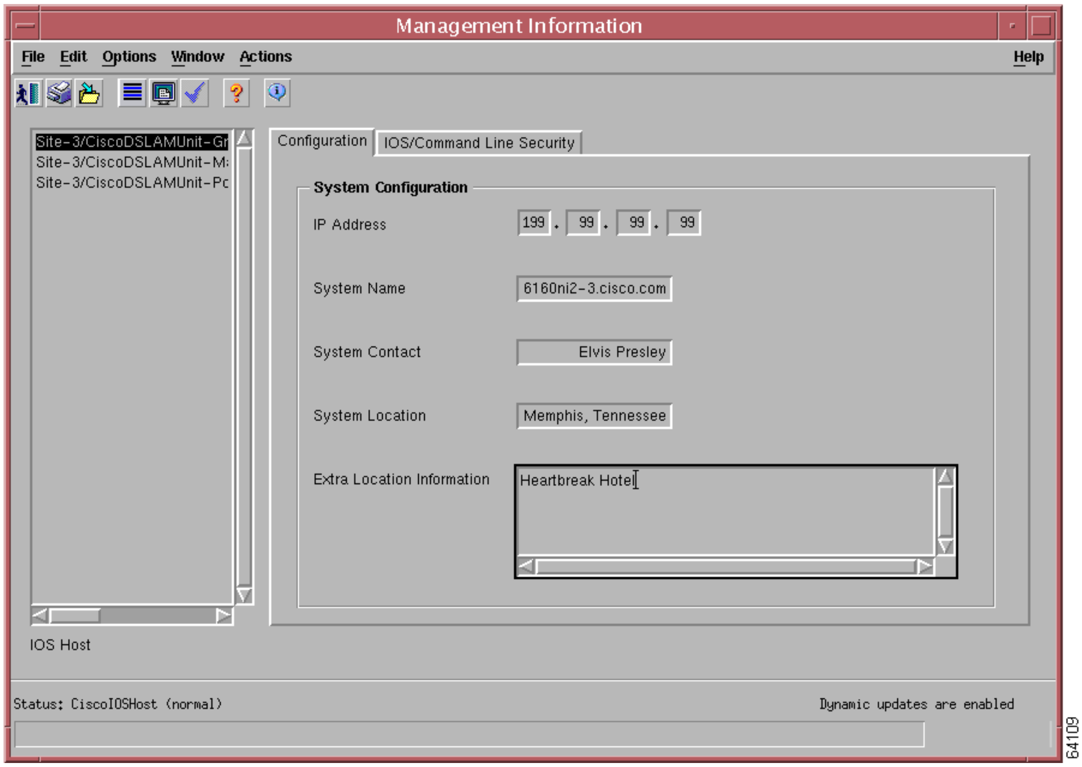
To enter chassis Cisco IOS command line security information, follow these steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the chassis for which you want to set security information to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > IOS Settings** from the object menu.

The Management Information window opens. (See Figure 2-20.)

Figure 2-20 Management Information Window—Configuration Tab



Step 3 Enter the appropriate information in the fields on this tab, as follows:

a. In the IP Address field, verify the IP address of the chassis for which you are setting the security password.

Do not change the chassis IP address from this window; this field is display only.

b. In the System Name field, verify the name of the system; this field is display only.

c. In the System Contact field, enter the name of the person or persons who are responsible for the network equipment.

d. In the System Location field, enter the physical location of the network equipment.

e. In the Extra Location Information field, enter additional physical location information for the network equipment.

Step 4 Verify the information in the Configuration tab.

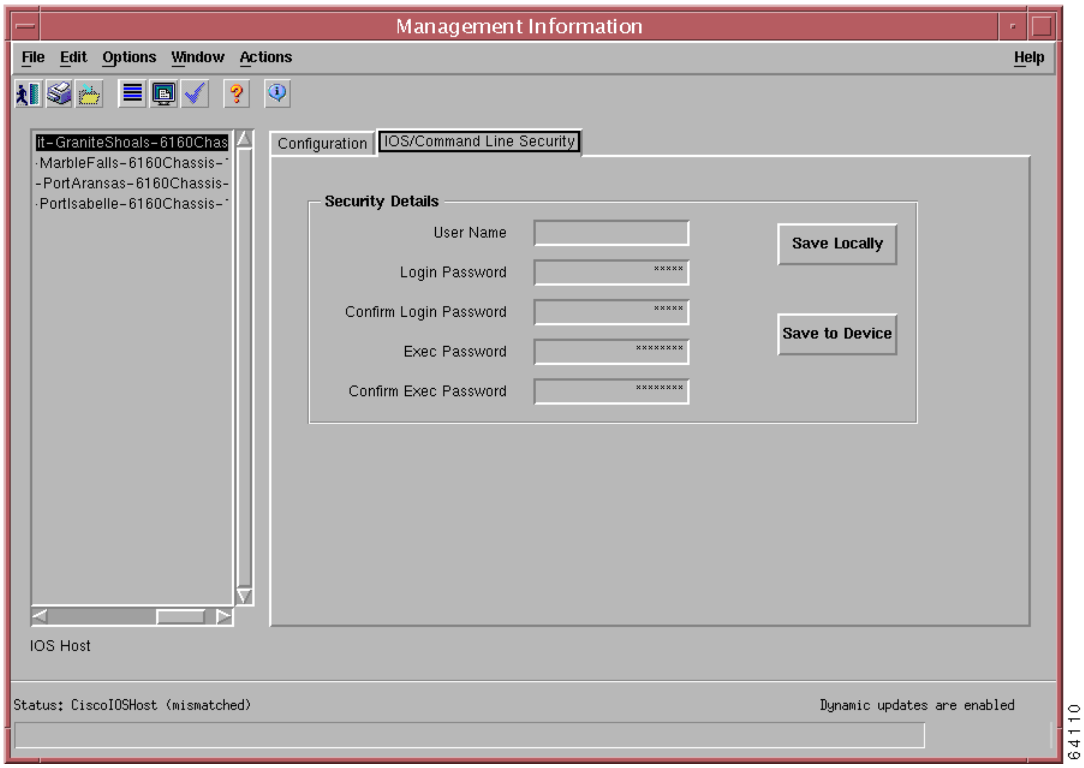
Setting the Cisco IOS Command Line Security Password

Complete these steps to set the Cisco IOS CLI security password:

Step 1 Click the **IOS/Command Line Security** tab.

The IOS Command Line Security tab becomes active. (See Figure 2-21.)

Figure 2-21 Management Information Window—IOS/Command Line Security Tab



Step 2 Enter the Cisco IOS command line security information as follows:

a. Do not enter a user name in the User Name field.

Generally a user name is not set on the node, so you should leave this field blank. Setting a user name allows that user and only that user to log in through the Telnet window and use IOS CLI commands from CDM to the DSLAM.

b. In the Login Password field, enter the login password.

This is the password that users will enter to use the IOS CLI from CDM through a telnet window. The login password entered in this field should match the login password on the Cisco DSLAM.

c. In the Exec Password field, enter your Cisco IOS CLI password.

This is the enable password that allows you to configure the elements on the network. The password that you enter in this field should match the privileged IOS password on the Cisco DSLAM.

Step 3 Click **Save Locally** to save your passwords locally in Cisco EMF and CDM.

Step 4 Click **Save to Device** to save the passwords on the selected DSLAM.

> **Note** When you click the Save to Device button, CDM saves the information locally *and* on the device.

An Action Report window opens and displays "Security details saved successfully."

Step 5 Click **Save** to save changes or **Close** to cancel.

Commissioning the DSLAM and other Network Elements

This section includes the following topics:

- Commissioning a Cisco DSLAM Chassis, page 2-31
- Commissioning Cards, page 2-35

Before you can begin actively managing the elements on your network, you must commission the objects that you have deployed. After you commission the chassis, CDM can collect alarm, performance, and status data for the chassis and the cards that are installed in the chassis.

The initial status of a commissioned chassis is Normal. The initial status for a commissioned card is either Normal or Preprovisioned if the physical card is not detected in the chassis. See the "Configuring or Querying Network Components and Using Hierarchical Levels" section on page 1-4 for more information about network object states.

Commissioning a Cisco DSLAM Chassis

When you commission a chassis, the chassis and all of its associated objects (that is, cards and interfaces) become available for management on the network. You can manually commission associated objects after you have already commissioned a chassis, or you can allow CDM to automatically commission the associated objects. For example, if you add a card after you have commissioned a chassis, the chassis automatically commissions itself during the next polling cycle (approximately 20 to 30 seconds).

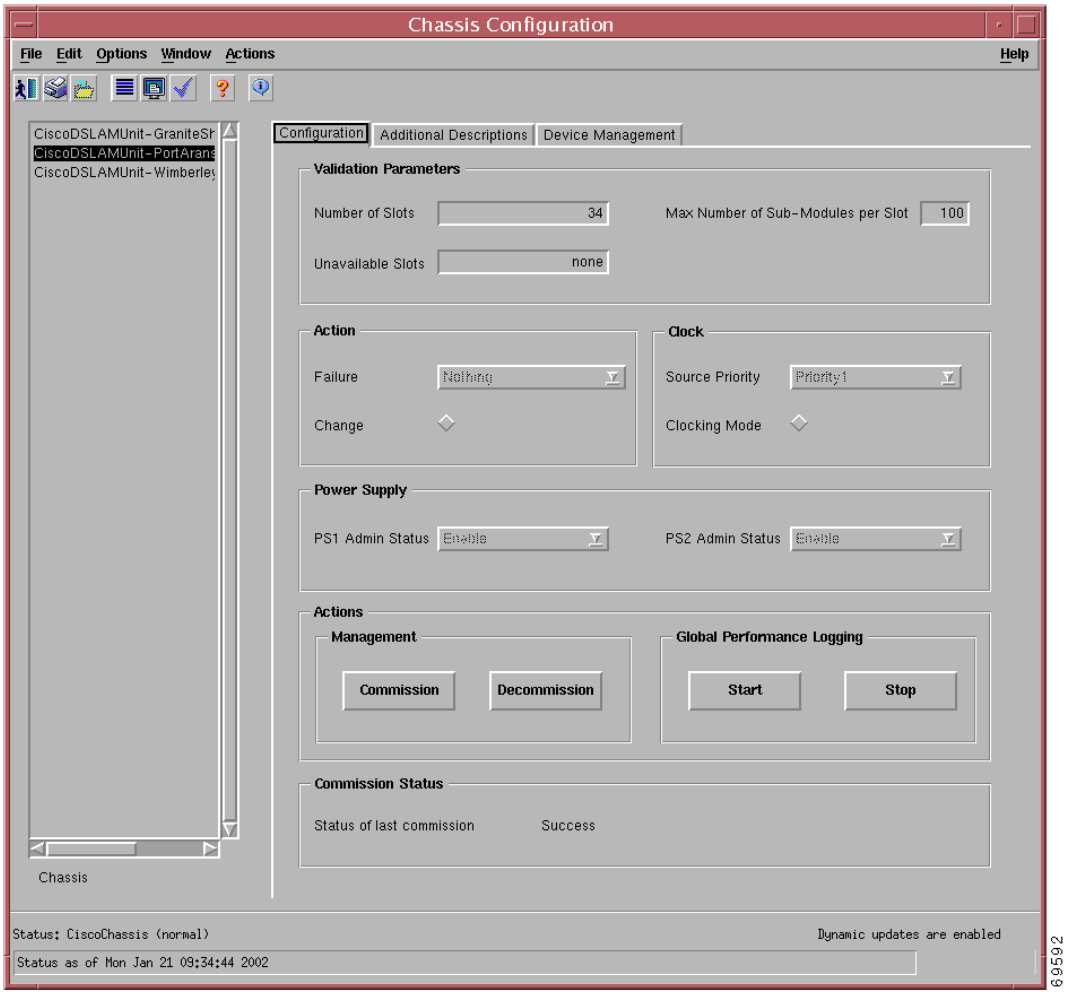
To commission a DSLAM chassis, follow these steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the chassis you want to commission to open the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Configuration** from the object menu.

The Chassis Configuration window opens to the Configuration tab. (See Figure 2-22.)

Figure 2-22 Chassis Configuration Window—Configuration Tab



Step 3 Click **Commission**.

The Chassis Configuration window Configuration tab includes the following areas, which are described in Table 2-5:

- Validation Parameters
- Action
- Clock
- Power Supply
- Actions
  - Management
  - Global Performance Logging
- Commission Status

Table 2-5 Chassis Configuration Window Field Descriptions

Field	Description
Validation Parameters	
Number of Slots	Displays the number of slots in the DSLAM.
Unavailable Slots	Displays the number of slots that are unavailable for management on the network.
Max Number of Sub-Modules per Slot	Identifies the number of submodules per slot.
Action	
Failure	Use the down arrow to identify the type of action that you want a failure to initiate, as follows: • Nothing • SendTrap • Shutdown • Send Trap and Shutdown
Change	Select this diamond if you want to change the reason for failure.
Clock	
Source Priority	Not used.
Clocking Mode	Not used.
Power Supply	
PS1 Admin Status	Not used.
PS2 Admin Status	Not used.
Actions	
Management	Click Commission to commission an object, or click Decommission to decommission an object. **Note** You must first decommission an object before you can delete it.
Global Performance Logging	Click Start to begin global performance logging, or click Stop to suspend global performance logging.
Commission Status	
Status of last commission	Displays Success or Failed after you click the Commission button.

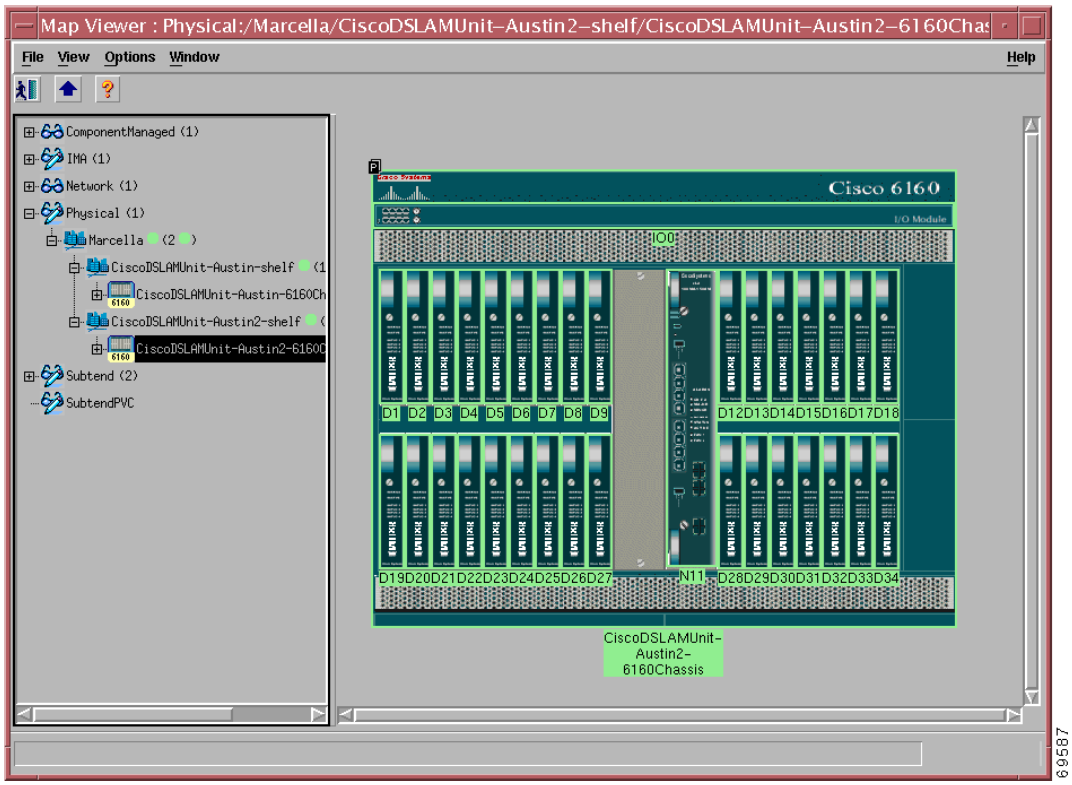
When you click Commission, CDM performs the following functions:

- Commissions the chassis
- Commissions the cards in the chassis
- Begins the subrack discovery process, discovering the objects below the chassis level

  During subrack discovery, CDM examines the chassis and automatically discovers and commissions the various interfaces on the cards in the chassis.

Note Cisco recommends that after you click **Commission**, you look at the Map Viewer window and monitor the Physical view as the software populates the chassis objects. As the software populates the objects, icons display on the right side of the window. If a card icon contains a lock symbol on the upper left side of the icon, the card is preprovisioned, that is, not physically present in the chassis and therefore not able to be managed. An example of this view is shown in Figure 2-23.

Figure 2-23 Example of a Commissioned Chassis



The icon that displays in the upper left corner of the chassis indicates the state of the chassis:

- Decommissioned—The chassis bitmap appears with hash marks.
- Normal—A “P” displays.
- Synchronizing—An “I” displays.

Note For more detailed information about object states, refer to the appendix about map states and icons in the *Cisco Element Management Framework User Guide*.

Commissioning Cards

When you commission a chassis, the chassis and all of its associated objects (that is, cards and interfaces), become available for management on the network. However, if you add a card or interface to the chassis after you have already commissioned the chassis, you can manually commission that card.

Note You can save time by allowing the chassis to automatically commission its objects during the polling cycles, rather than manually commissioning a card or interface.

To commission a card, you use the Configuration window. From this window, you can also enter common location language identifier (CLLI) codes or text descriptions for each card in the chassis.

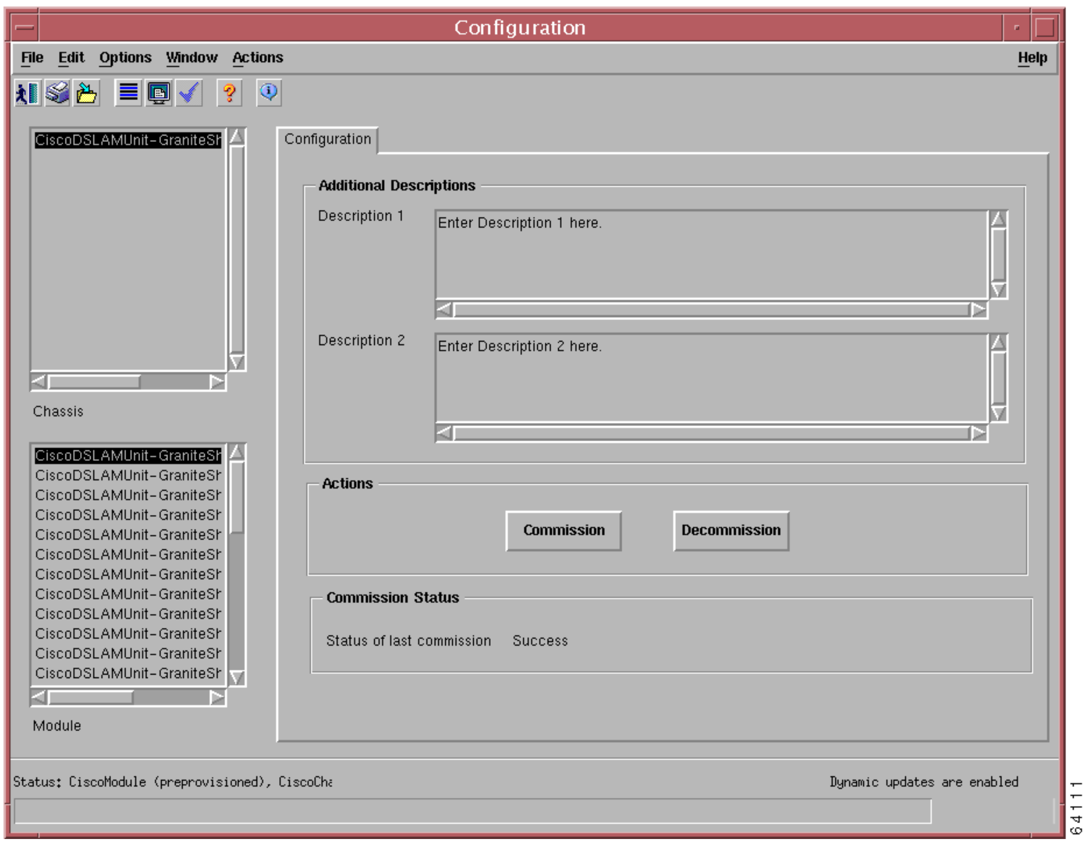
To open the Configuration window and commission a card, follow these steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the NI-2 card or the line card that you want to commission.

Step 2 Choose **Cisco DSL Manager > Module > Configuration** from the object menu.

The Configuration window opens. (See Figure 2-24.)

Figure 2-24 Configuration Window



Step 3 Select the chassis and card from the list box on the left side of the window.

Step 4 Enter CLLI codes or other text descriptions in the Description 1 and Description 2 fields.

CDM saves the information that you enter in these fields, but not to the hardware. After you enter a description, CDM displays the descriptive text each time a user selects the object with which a description is associated.

Step 5 Click **Commission** to commission the card, or click **Decommission** to decommission the card.

The status of the commission process displays at the bottom of the window in the Status field.

Step 6 Click **Save** in the toolbar, or choose **File > Save**.

Configuring Interfaces

This section includes the following topics:

Note The OC-3 and DS3 interfaces are not configurable from the CDM GUI.

Configuring ATM Interfaces

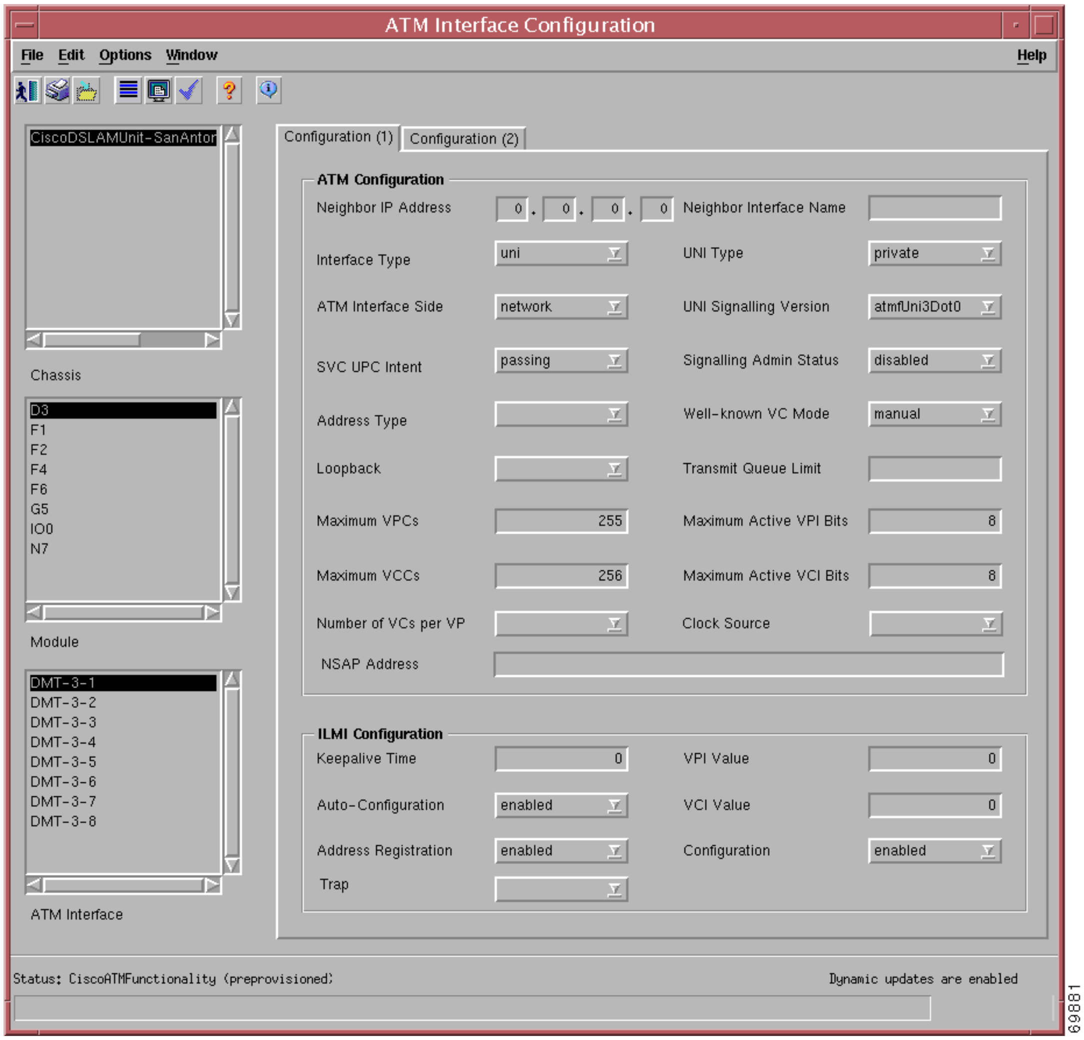
Complete the following steps to configure ATM interfaces:

Step 1 From the left side of the Map Viewer window, right-click the interface for which you want to configure ATM properties.

Step 2 Chose **Cisco DSL Manager > Interface > Configuration > ATM** from the object menu.

The ATM Interface Configuration window opens to the Configuration (1) tab (see Figure 2-25).

Figure 2-25 ATM Interface Configuration Window—Configuration (1) Tab



Step 3 Refer to the descriptions of the fields in this window to set the ATM configuration fields. (See Table 2-6 and Table 2-7.)

The ATM Interface Configuration window has two tabs—Configuration (1) and Configuration (2). The fields on the Configuration (1) tab are described in Table 2-6. This tab has two areas—ATM Configuration and Interim Link Management Interface (ILMI) Configuration.

Table 2-6 ATM Configuration Window Configuration (1) Tab Field Descriptions

Field	Description
ATM Configuration	
Neighbor IP Address	Enter the IP address of the neighbor system that is connected to the far end of this interface and to which the network management system can send SNMP messages. This is only available when the chassis are managed though inband management.
Interface Type	Use the down arrow to specify the type of ATM interface: UNI[1] (User to Network), PNNI[2], IISP[3], or NNI PVC only. To modify the interface type, the interface administrative status has to be down and interface Ilmi autoconfiguration must be disabled.
ATM Interface Side	Use the down arrow to specify whether ATM interface is subscriber (user) side or network side. Select notApplicable to specify that the interface type is other than uni or iisp.
SVC UPC[4] Intent	Use the down arrow to specify the type of UPC to use on the destination half-leg of soft PVCs: passing, tagging, or dropping. Values other than passing are allowed only if policing is supported on the interface.
Address Type	Use the down arrow to specify the type of ATM addresses on this interface: nsap, es1, e164, or null. Only null or NSAP are supported in this version. If you select NSAP you must also specify the NSAP address.
Loopback	Use the down arrow to specify to the loopback mode: • line enabled: Packets are transmitted back to the source to test interface functionality and ensure that packets transmitted through the interface reach the destination without data loss. • no loopback (disabled): Restricts connection status (success or failure) messages from being received. • diagnostic: The transmit data stream is looped to the transmit direction.
Maximum VPCs[5]	Enter the maximum number of PVCs and SPVCs that are supported for this interface.
Maximum VCCs[6]	Enter the maximum number of PVCs and SPVCs that are supported for this interface.
Number of VCs per VP	Use the down arrow to set the number of virtual channels per virtual path.
NSAP[7] Address	Enter the NSAP address.
Neighbor Interface Name	Enter the name of the connected interface on the neighbor system at the far end of this interface, to which the network management system can send SNMP messages. This is only available when the chassis are managed though inband management.
UNI Type	Use the down arrow to specify the type of UNI type, either private or public. Only specify this field if the ATM interface type is UNI.

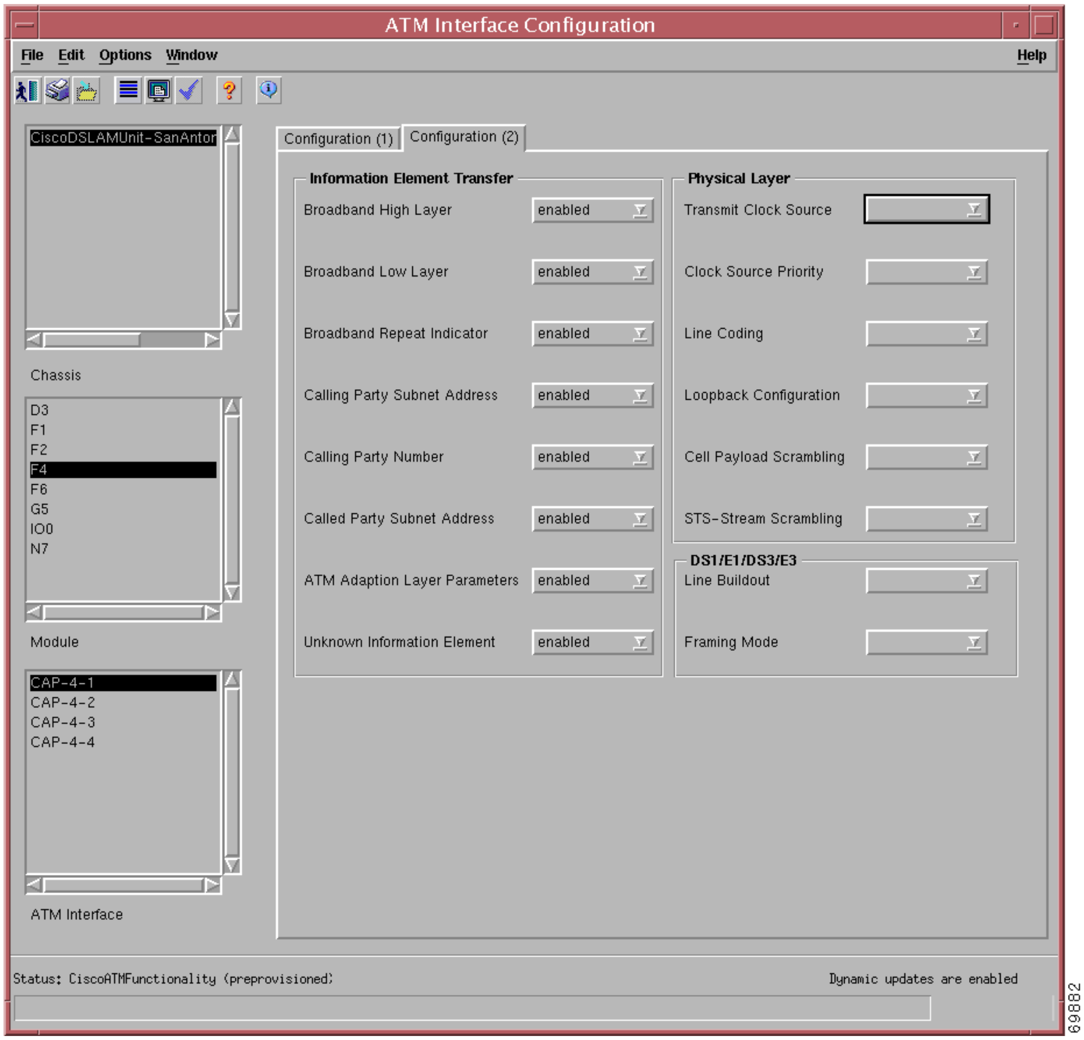
Table 2-6 ATM Configuration Window Configuration (1) Tab Field Descriptions (continued)

Field	Description
UNI Signalling Version	Use the down arrow to specify the version of UNI signalling that is currently being used on the UNI or IISP interface: atmfUni3Dot0, atmfUni3Dot1, or atmfUni4Dot0. Choose **Not applicable** when the interface is a PNNI interface or when signalling is disabled. To change the setting in this field, the interface admin status must be down and the interface Ilmi autoconfiguration disabled.
Signalling Admin Status	Use the down arrow to enable or disable signalling/sscop[8] on this interface. Choose **disable** to clear all the active SVCs on this interface.
Well-known VC Mode	Use the down arrow to specify whether well-known VCs should be created automatically or manually on the interface.
Transmit Queue Limit	Enter the transmit length.
Maximum Active VPI Bits	Enter the maximum number of active VPI bits configured for use on this interface.
Maximum Active VCI Bits	Enter the maximum number of active VCI bits configured for use on this interface.
Clock Source	Use the down arrow to specify the type of clock source, either none or internal.
ILMI Configuration	
Keepalive Time	Enter the 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.
Auto-Configuration	Use the down arrow to enable or disable the ILMI link and interface type determination. The configuration takes effect only on the next interface restart.
Address Registration	Use the down arrow to enable or disable ILMI address Registration on this interface. The configuration takes effect only on the next interface restart.
Trap	Use the down arrow to enable or disable traps for this interface.
VPI Value	Enter the VPI value of the VCC that supports the ILMI for this interface. If the VPI Value is set to 0, the ILMI will be disabled.
VCI Value	Enter the VCI value of the VCC that supports the ILMI for this interface. If the VCI Value is set to 0, the ILMI will be disabled.
Configuration	Use the down arrow to 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.

1. UNI = user to network
2. PNNI = private network to network
3. IISP = interim interface signalling protocol
4. UPC = usage parameter control
5. VPCs = virtual path connections
6. VCCs = virtual circuit connections
7. NSAP = Network Service Access Point
8. SSCOP = Service Specific Connection Oriented Protocol

The Configuration (2) tab has three areas—Information Element Transfer, Physical Layer, and DS1/E1/DS3/E3. This tab is shown in Figure 2-26.

Figure 2-26 ATM Configuration Window Configuration (2) Tab



The fields on the Configuration (2) tab are described in Table 2-7.

Table 2-7 ATM Configuration Window Configuration (2) Tab Field Descriptions

Field	Description
Information Element Transfer	
Broadband High Layer	Use the down arrow to enable or disable to accept, transfer, and deliver the Broadband High Layer information element from the calling party to the called party.
Broadband Low Layer	Use the down arrow to enable or disable to accept, transfer, and deliver the Broadband Low Layer information element from the calling party to the called party.

Table 2-7 ATM Configuration Window Configuration (2) Tab Field Descriptions (continued)

Field	Description
Broadband Repeat Indicator	Use the down arrow to enable or disable to accept, transfer, and deliver the Broadband Repeat Indicator information element from the calling party to the called party. This object shall only be transferred if the Broadband Low Layer is enabled.
Calling Party Subnet Address	Use the down arrow to enable or disable to accept and transfer the calling party subaddress information.
Calling Party Number	Use the down arrow to enable or disable the calling party number information element is transferred to the called party.
Called Party Subnet Address	Use the down arrow to enable or disable to accept, transfer, and deliver called party subaddress information.
ATM Adaptation Layer Parameters	Use the down arrow to enable or disable to accept, transfer, and deliver the ATM adaption layer parameters.
Unknown Information Element	Use the down arrow to enable or disable to accept, transfer, and deliver the unknown Information Element from the calling party to the called party.
Physical Layer	
Transmit Clock Source	Use the down arrow to specify the source of the transmit clock: • loopTiming—The recovered receive clock is used as the transmit clock. • freeRunning—A local clock source is used. • networkDerived—The recovered receive clock from another interface is used as the transmit clock source.
Clock Source Priority	Use the down arrow to set the priority of this interface if configured as a network clock source: notConfigured, priority1, priority2, priority3, priority4. notConfigured indicates this is not configured as a network clock source.
Line Coding	Use the down arrow to specify the line coding that is present on the physical interface (applies to DS1/E1 interfaces only): • ami[1] on the DS1/E1 interface. • b8zs indicates B8ZS[2] line code on DS1 interfaces. • hdb3 indicates HDB3[3] line code on E1 interfaces.
Loopback Configuration	Use the down arrow to specify the loopback configuration on the physical interface: • noLoop indicates no loopback is present. • diagnosticLoop indicates transmit data stream is looped to the receive direction. • lineLoop indicates receive data stream is looped to the transmit direction.
Cell Payload Scrambling	Use the down arrow to set cell payload scrambling to on or off.
STS-Stream Scrambling	Use the down arrow set STS[4]-stream scrambling to on or off.

Table 2-7 ATM Configuration Window Configuration (2) Tab Field Descriptions (continued)

Field	Description
DS1/E1/DS3/E3	
Line Buildout (physical interfaces)	Use the down arrow to set the line buildout configuration on the transmit signal: • e3AllCables: all E3 interface cables. • ds3CablesUnder225: DS3 interface cables under 225 feet • ds3CablesOver225: DS3 interface cables over 225 feet • ds1Cables0To110: DS1 interface cables 0 to 110 feet • ds1Cables110To220: DS1 interface cables 110 to 220 feet • ds1Cables220To330: DS1 interface cables 220 to 330 fee • ds1Cables330To440: DS1 interface cables 330 to 440 feet • ds1Cables440To550: DS1 interface cables 440 to 550 feet • ds1Cables550To660: DS1 interface cables 550 to 660 feet • ds1CablesOver600: DS1 interface cables over 600 feet • e1AllCables: all E1 interface cables
Framing Mode (physical interfaces)	Use the down arrow to set the framing format: • sonet: sts-3c (OC-3) or sts-12c format (OC-12) • sdh indicates stm1 (OC-3) or stm4 (OC-12) • ds3m23adm indicates M23 ADM[5] mode; applies to DS3 interfaces • ds3m23plcp indicates M23 PLCP[6] mode; applies to DS3 interfaces • ds3cbitadm indicates C-BIT ADM mode; applies to DS3 interfaces • ds3cbitplcp indicates C-BIT PLCP mode; applies to DS3 interfaces • e3g832adm indicates G.832 ADM mode; applies to E3 interfaces • e3g751adm indicates G.751 ADM mode; applies to E3 interfaces • e3g751plcp indicates G.751 PLCP mode; applies to E3 interfaces • ds1sfadm indicates DS1 SF ADM mode; applies to DS1 interfaces • ds1esfadm indicates DS1 ESF ADM mode; applies to DS1 interfaces • ds1sfplcp indicates DS1 SF PLCP mode; applies to DS1 interfaces • ds1esfplcp indicates DS1 ESF PLCP mode; applies to DS1 interfaces • e1adm indicates E1 ADM mode; applies to E1 interfaces • e1plcp indicates E1 PLCP mode; applies to E1 interfaces • e1crcadm indicates E1 CRC-4 ADM mode; applies to E1 interfaces • e1crcplcp indicates E1 CRC-4 PLCP mode; applies to E1 interfaces

1. AMI = alternate mark inversion
2. B8ZS = bipolar with 8 zero substitution
3. HDB3 = high density bipolar 3
4. STS = synchronous transport signal
5. ADM = add/drop multiplexer
6. PLCP = physical layer convergence protocol

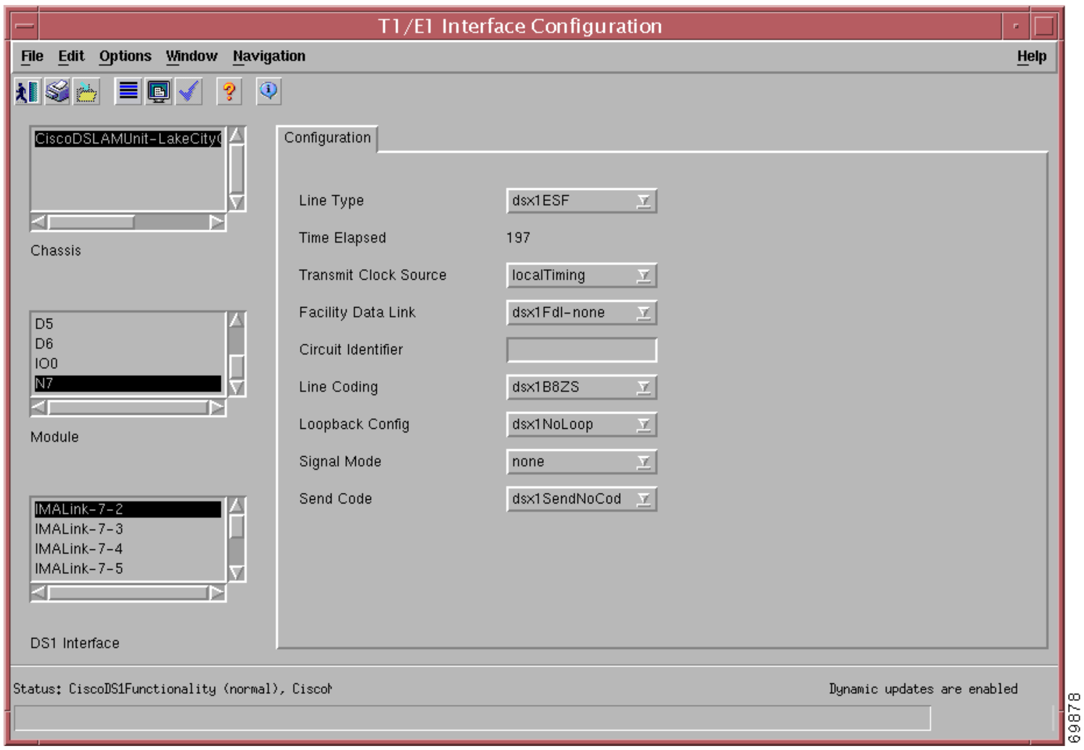
Configuring the T1/E1 Interface

Complete the following steps to configure a DS1 (T1/E1) interface:

Step 1 From the left side of the Map Viewer window, right-click the DSLAM whose DS1 interface you want to configure and choose **Cisco DSL Manager > Interface > T1/E1**.

The T1/E1 Interface Configuration window opens (see Figure 2-27).

Figure 2-27 T1/E1 Interface Configuration Window



Step 2 Select the NI card from the list box on the left to set the parameters for this interface.

The T1/E1 Interface Configuration window has one tab, Configuration. The fields on this tab are described in Table 2-8.

Table 2-8 T1/E1 Interface Configuration Window

Field	Description
Line Type	Use the down arrow to choose the type of line for this circuit: • dsx1ESF[1] • dsx1D4[2] • dsx1E1 • dsx1E1-CRC[3] • dsx1E1-MF[4] • dsx1E1-CRC-MF
Time Elapsed	Displays the number of seconds that have elapsed since the beginning of the current measurement period.
Transmit Clock Source	Use the down arrow to choose the transmit clock source: • loopTiming • localTiming • throughTiming
Facility Data Link	Use the down arrow to choose the type of zero code suppression to be used on this circuit: • other • dsx1Ansi-T1-403 • dsx1Att-54016 • dsx1Fdl-none
Circuit Identifier	Displays the transmission vendor’s circuit ID.
Line Coding	Use the down arrow to choose the line coding: • JBZS • B8ZS[5] • HDB3[6] • ZBTSI[7] • AMI[8] • other
Loopback Config	Use the down arrow to choose the loopback configuration type: • dsx1NoLoop • dsx1PayloadLoop • dsx1LineLoop • dsx1otherLoop

Table 2-8 T1/E1 Interface Configuration Window (continued)

Field	Description
Signal Mode	Use the down arrow to choose the type of signal mode: • none • robbedBit • bitOriented • messageOriented
Send Code	Use the down arrow to choose the type of code to be sent across the DS1 interface: • dsx1SendNoCode • dsx1SendLineCode • dsx1SendPayloadCode • dsx1SendResetCode • dsx1SendQRS • dsx1Send511Patttern • dsx1Send3in24Pattern • dsx1SendOtherTestPattern

1. ESF = extended super frame or extended superframe format
2. D4 = 4th generation channel back
3. CRC = cyclic redundancy check
4. MF = multiframe
5. B8ZS = bipolar with 8 zero substitution
6. HBD3 = high density bipolar 3
7. ZBTSI = zero byte time slot interchange
8. AMI = alternate mark inversion

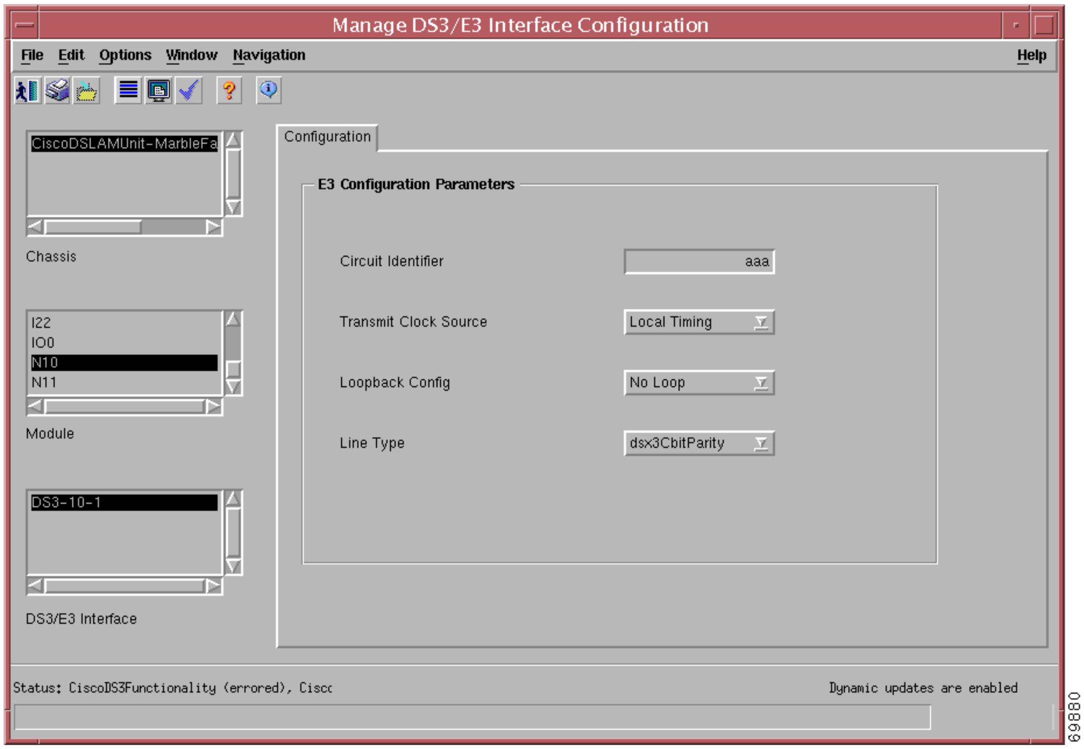
Configuring an E3 Interface

Complete the following steps to configure an E3 interface.

Step 1 From the left side of the Map Viewer window, right-click the DSLAM whose E3 interface you want to configure and choose **Cisco DSL Manager > Interface > E3**.

The Manage DS3/E3 Interface Configuration window opens (see Figure 2-28).

Figure 2-28 Manage DS3/E3 Interface Configuration Window



Step 2 Select the NI card from the list box on the left to set the parameters for this interface.

Step 3 Set the fields as described in Table 2-9.

The DS3/E3 Interface Configuration window has one tab, Configuration and one area, E3 Configuration Parameters. The fields on this tab are described in Table 2-9.

Table 2-9 DS3/E3 Interface Configuration Window

Field	Description
Circuit Identifier	Displays the circuit ID for the interface.
Transmit Clock Source	Use the down arrow to choose the type of transmit clock source: • LoopTiming • LocalTiming

Table 2-9 DS3/E3 Interface Configuration Window (continued)

Field	Description
Loopback Config	Use the down arrow to choose the type of loopback configuration: • No Loop • Payload Loop • Line Loop • Other Loop
Line Type	Use the down arrow to set the line type: • dsx3Cbit Parity • e3other • e3Framed • e3Plcp[1]

1. PLCP = Physical Layer Convergence Protocol

Enabling SNMP Trap Generation

In the SNMP Management window, you can enable or disable trap generation on a selected device. You can also verify and modify the SNMP version and read or write names for a selected device from this window.

Note Use this window to *modify* SNMP information. You must *set* SNMP information when you deploy the chassis (see the "Manually Deploying a Cisco DSLAM Chassis" section on page 2-13). Otherwise, CDM is unable to commission the chassis that you are configuring.

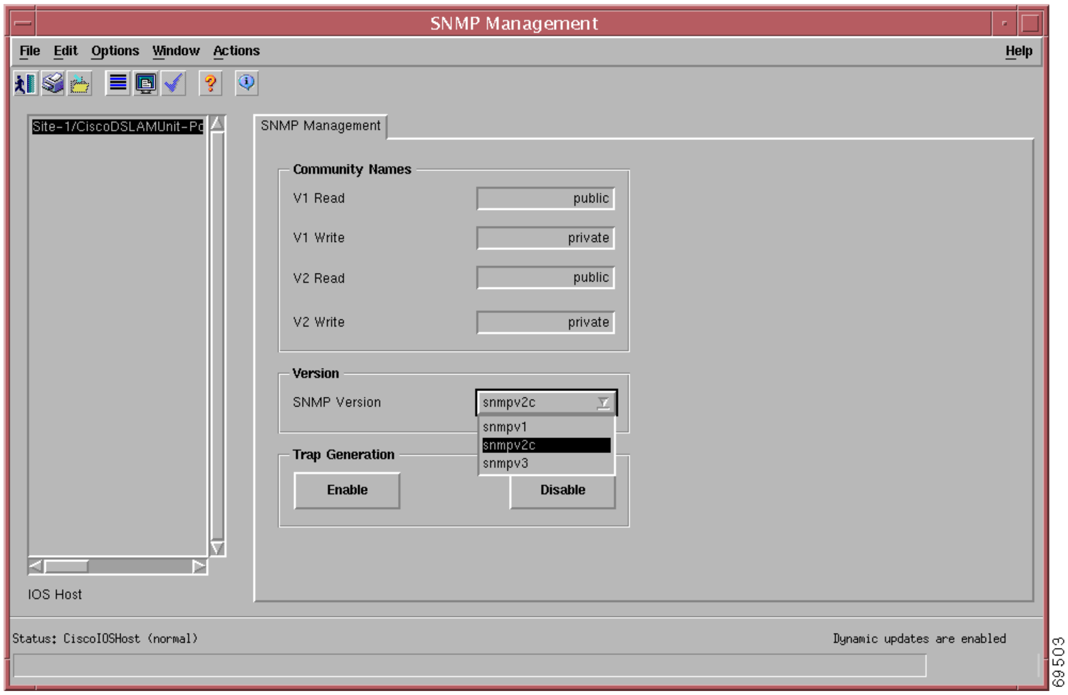
To open the SNMP Management window and enable SNMP trap generation, follow these steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the chassis for which you want to set SNMP traps.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > SNMP Settings** from the object menu.

The SNMP Management window opens. (See Figure 2-29.)

Figure 2-29 SNMP Management Window



The chassis that you selected in the previous step is highlighted in the list box on the left side of the window. The SNMP Management window contains four areas of information:

- Community Names
- Version
- Trap Generation

When you open the SNMP Management window, CDM populates the fields to display the SNMP parameters that are set when you deploy that DSLAM. CDM does not currently support SNMP Version 3.

Step 3 In the Trap Generation field, click **Enable** or **Disable**.

You can enable or disable trap generation by clicking the appropriate button. When trap generation is enabled on a selected chassis, any traps generate alarms and send them to the IP address of the specified chassis. This means that alarms are visible to the user in the appropriate view of CDM. You can also disable this feature, so that no traps are generated and no alarms are sent. This means that no alarms are visible to the user on the selected chassis.

Deleting Network Elements

You can delete Cisco DSLAM chassis or line cards from most active windows, or by selecting an object from the left side of the Map Viewer window. When you delete a chassis, you delete all cards, interfaces, connections, and profiles within that chassis. You can only delete a chassis if it is decommissioned (has never been commissioned or has been decommissioned), which means that CDM is no longer actively managing the chassis.

Before you can delete a chassis, a module, or a line card from CDM, you must first decommission it, as follows.

Caution If a module or line card has never been commissioned, do not decommission it before you delete it. An example is a preprovisioned line card that does not physically exist on the hardware but that is present in CDM. Because it does not physically exist in the DSLAM, you should not decommission it before you delete it. Rather, use the steps for deletion described in the following section to delete it from CDM. If you try to decommission it first, problems will occur.

Step 1 From the left side of the Map Viewer window, right-click the chassis or other object that you want to delete.

Step 2 Choose the appropriate menu options to open the appropriate Configuration window:

a. Choose **Cisco DSL Manager > Chassis > Configuration** from the object menu to open the Chassis Configuration window (see Figure 2-22 on page 2-32) and decommission a chassis.

b. Choose **Cisco DSL Manager > Module > Configuration** from the object menu to open the Configuration window (see Figure 2-24 on page 2-35) and decommission a module.

Step 3 Click **Decommission** in the related Configuration window.

Step 4 Verify that the chassis, module, or line card is decommissioned in the Status field.

After CDM has successfully decommissioned the chassis, module, or interface, you can delete it as follows:

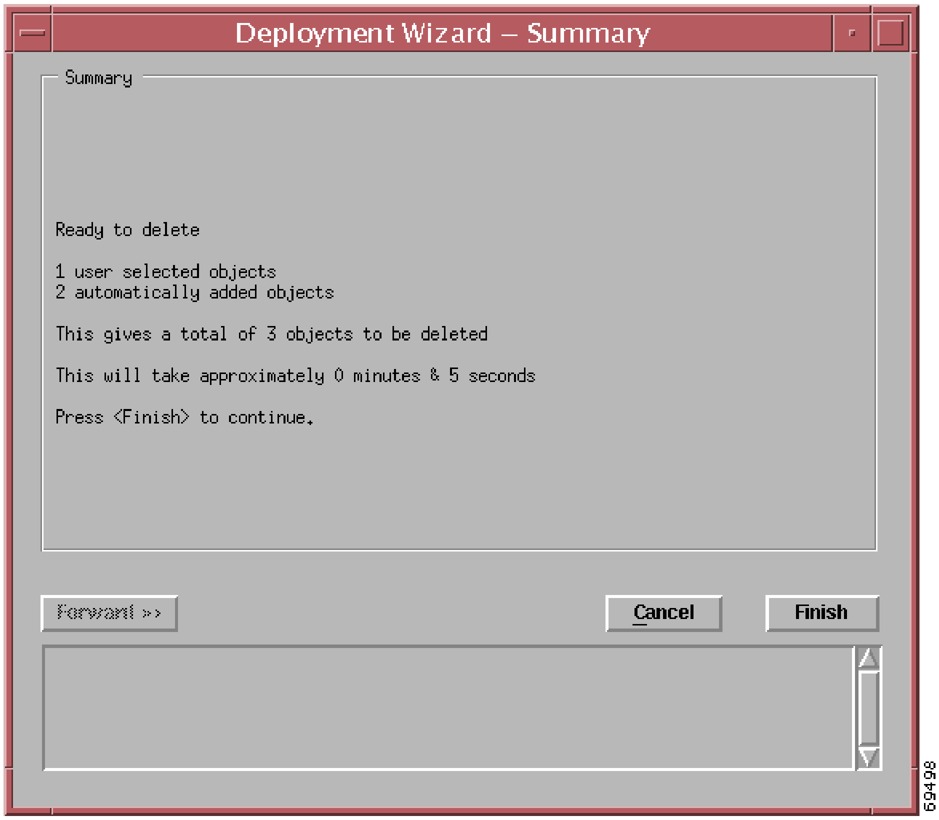
Step 1 From the left side of the Map Viewer window, right-click the chassis, module, or interface to open the object menu.

Step 2 Choose **Deployment > Delete Objects** from the object menu.

Note You can also select a chassis to be deleted from the list box in an active window, such as the Chassis Configuration window, and then select **Deployment > Delete Objects**.

The Deployment Wizard—Summary window opens. (See Figure 2-30.)

Figure 2-30 Deployment Wizard Summary Window—Delete Object



Step 3 Click **Finish** to delete the selected chassis, module, or interface (or click **Cancel** to abort the process).

After you click **Finish**, CDM informs you whether the deletion was successful.

Creating and Applying *x*DSL Profiles

This chapter describes how to create, apply, and delete *x*DSL subscriber profiles.

This chapter includes the following sections:

Introduction to Using *x*DSL Profiles

You use *x*DSL profiles to apply a set of existing values (parameters) to several objects of the same type. Using profiles saves you from having to enter the same data many times. After you create a profile, you can apply it to other subscriber lines. CDM provides a default *x*DSL profile that includes specific parameters for each type of line card; the default profile is resident on the DSLAM.

You can also copy and alter the default parameters to create new *x*DSL profiles. You can change the parameters for one type of line card and save this *x*DSL profile with a new name; the parameters for the other line cards remain at the default settings unless you also change them.

CDM provides the following types of *x*DSL profile configurations:

- Asymmetric digital subscriber line (ADSL) profiles:
  - Discrete multitone (DMT) profiles
  - Carrierless amplitude and phase modulation (CAP) profiles
- Symmetrical digital subscriber line (SDSL) profiles, including G.SHDSL

When you add a subscriber, you perform the following tasks:

- Create and apply a profile to a subscriber line.
- Deploy a PVC or SPVC, then apply a QoS profile and connect it.

In CDM, a subscriber profile specifies the parameters of a subscriber line, which has a PVC or SPVC with two VCLs at each end. See Chapter 4, "Creating Connections and ATM QoS Profiles," for instructions on how to create connections and use ATM QoS profiles.

Roadmap for Creating and Applying Profiles and Establishing Connections

The process for creating and applying profiles and establishing subscriber connections is as follows:

1. Access the object menu for the chassis, module, or interface object to which you want to associate an *x*DSL profile.
2. Choose the existing *x*DSL profile parameters that the DSLAM contains or create new parameters.
3. Apply an existing, uploaded profile or a newly created set of parameters to the subscriber line unless you want to use the default *x*DSL profile for that type of line card.
4. Deploy a PVC or SPVC object in CDM, apply a QoS profile, and make the connection.

Note If the deployment fails, you can upload the ATM profile. See the "Manually Uploading ATM QoS Profiles" section on page 4-49 for instructions.

5. (Optional) Start performance polling on the connection.

Overview of Using *x*DSL Profiles

The state of the DSLAM chassis and module determines how you can use *x*DSL profiles. Before you sync, create, apply, or delete *x*DSL profiles, review the guidelines described in Table 3-1.

Table 3-1 Guidelines for Using Profiles

<table>
<tr><th>Chassis or Module State</th><th>Profile Guidelines</th></tr>
<tr><td>Chassis and module in normal state (not decommissioned)</td><td>You can:
Create profiles
Apply profiles
Modify applied profiles
Modify unapplied profiles
Delete unapplied profiles; this removes the profile from the DSLAM node and IOS device.
You cannot delete applied profiles.</td></tr>
<tr><td>Chassis in normal state and module is decommissioned</td><td>You can:
Create profiles
Modify applied profiles
Modify unapplied profiles
Delete unapplied profiles
You cannot:
Apply profiles
Delete applied profiles</td></tr>
<tr><td>Chassis is decommissioned</td><td>You can:
Delete an unapplied profile, but only temporarily from CDM. The profile remains on the device and once the chassis is recommissioned, profile synchronization occurs resulting in the deleted profile reappearing on the chassis node.
Delete an applied profile but only temporarily from CDM. The profile remains on the device and once the chassis is recommissioned, profile synchronization occurs resulting in the deleted profile reappearing on the chassis node.
You cannot:
Create profiles
Apply profiles
Modify applied profiles
Modify unapplied profiles</td></tr>
</table>

Tip Here is a workaround for removing an applied *x*DSL profile from an interface or module port through the CDM GUI. Apply a default or another profile to the interface whose applied profile is the one that you want to delete. After CDM overwrites the applied profile with either the default profile or a different profile, you can delete the previously applied profile.

Using the Default *x*DSL Profile

Each Cisco DSLAM ships with an existing *x*DSL default profile on the DSLAM node. When you commission the DSLAM, CDM automatically uploads this profile. You can use the default *x*DSL profile, and you can create new ones. The following sections include instructions for creating new *x*DSL profiles by modifying the default *x*DSL profile and saving it with a new name.

The *x*DSL profile contains parameters for each type of line card—ADSL (DMT) and SDSL, G.SHDSL, and ADSL (CAP). To display the *x*DSL default profile that resides on a DSLAM, you can Telnet to the IP address of the DSLAM and enter the **show dsl profile default** command to display these defaults. An example follows:

```
dsl profile default:
    Link Traps Enabled: NO
    Alarms Enabled: NO
    ATM Payload Scrambling: Enabled

DMT profile parameters
    Maximum Bitrates:
    Interleave Path:   downstream:   640 kb/s,   upstream:   128 kb/s
    Fast Path:         downstream:     0 kb/s,   upstream:     0 kb/s
    Minimum Bitrates:
    Interleave Path:   downstream:     0 kb/s,   upstream:     0 kb/s
    Fast Path:         downstream:     0 kb/s,   upstream:     0 kb/s
    Margin:               downstream:     6 dB,     upstream:     6 dB
    Interleaving Delay:   downstream: 16000 usecs,  upstream: 16000 usecs
    Check Bytes (FEC):
    Interleave Path:   downstream:    16,        upstream:    16
    Fast Path:         downstream:     0,        upstream:     0
    R-S Codeword Size:    downstream:  auto,        upstream:  auto
    Trellis Coding:         Disabled
    Overhead Framing:       Mode 3
    Operating Mode:         Automatic
    Training Mode:          Quick
    Minrate blocking:       Disabled
    SNR Monitoring:         Disabled

SDSL profile parameters
    Maximum Bitrates: 784 kbps

SHDSL profile parameters
    Maximum Bitrates:          776 kbps
    SNR margin threshold:        3 dB
    SNR margin target:           0 dB
    SNR margin min:              0 dB
    Masktype:              symmetric
    Annex:                         A
```

```
CAP profile parameters
    Maximum Bitrates:      downstream:   640 kb/s,   upstream:    91 kb/s
    Minimum Bitrates:      downstream:     0 kb/s,   upstream:     0 kb/s
    Margin:                downstream:     3 dB,     upstream:     6 dB
    PSDM:                  downstream:   -40 dBm/Hz, upstream:   -38 dBm/Hz
    Interleaving Delay:      Long (Reed-Solomon enabled)
    136K Baud DS Rates:      Enabled
    68K Baud US Rates:       Disabled
    17K Baud US Rates:       Disabled
    CPE Signature:           0

IDSL profile parameters
    Bitrate:               128 kbit/sec
    Encapsulation:         llc-ppp
    Frame Relay parameters:
    UPC intent:            pass
    Bc default:            32768 bytes
    LMI type:              cisco
    lmi-n392dce:           2 events
    lmi-n393dce:           2 events
    lmi-t392dce:           15 seconds
```

Note CDM 3.4 does not manage or support IDSL line cards. However, you can create IDSL profiles through Cisco IOS.

After you have created new *x*DSL profiles, you can use the **show dsl profile** command to display a list of all *x*DSL profiles, including the default profiles and any new ones that you have created. If you want to display the parameters of a specific profile, use the command, **show dsl profile <name_of_profile>**.

Using the Sync Profile Feature

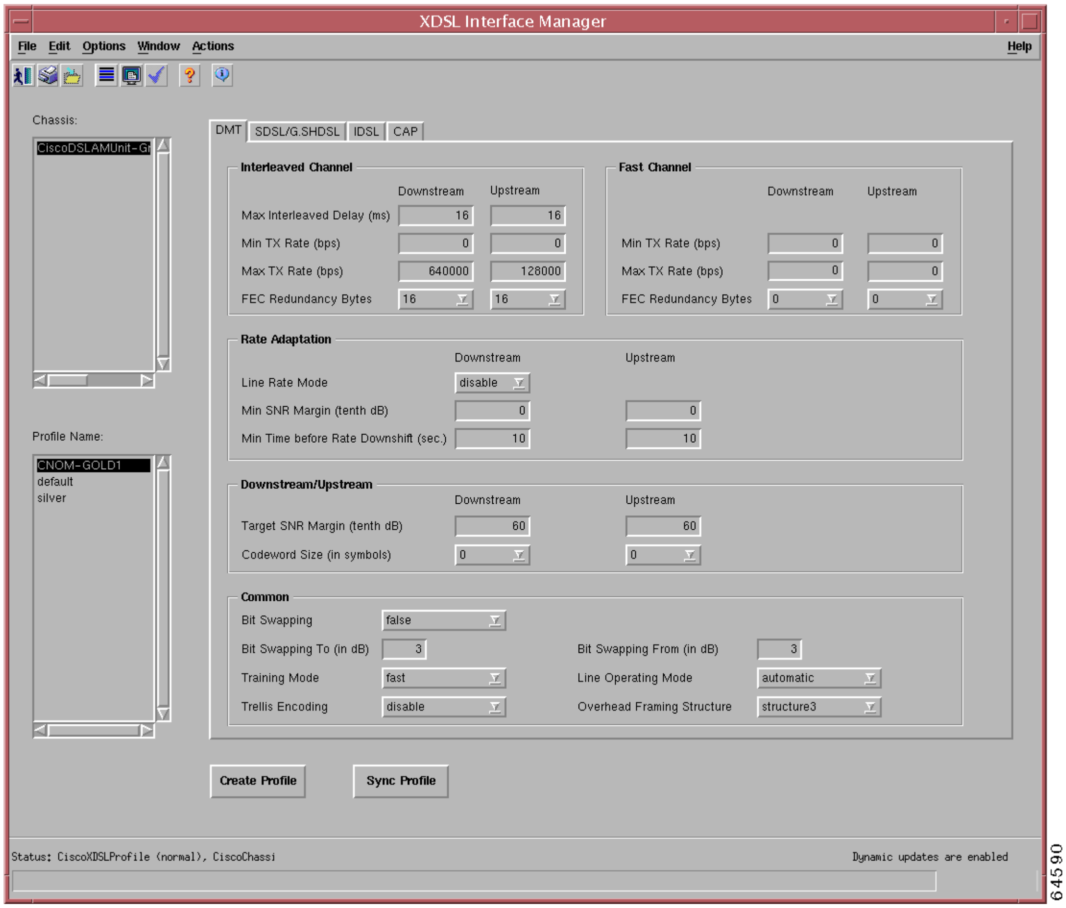
You can manually sync all of the profiles on a DSLAM or several DSLAMs by using the Sync Profile button. Complete these steps:

Step 1 On the left side of the Map Viewer window, right-click the DSLAM whose *x*DSL profiles you want to sync, or right-click the site if you want to sync profiles of several DSLAMs.

Step 2 Choose **Cisco DSL Manager > Chassis > Profile Management > *x*DSL Profiles**.

The XDSL Interface Manager window opens. (See Figure 3-3.)

Figure 3-1 XDSL Interface Manager Window



If you opened the XDSL Interface Manager window from one DSLAM, that DSLAM is highlighted in the list box on the left of the window.

Step 3 To sync the *x*DSL profiles for several DSLAMs, hold down the **Shift** key and highlight all of the chassis whose profiles you want to sync.

Step 4 Click **Sync Profile**.

A Notification Dialog window opens to notify you whether the synchronization process was successful.

Creating a New Profile from an Existing Profile

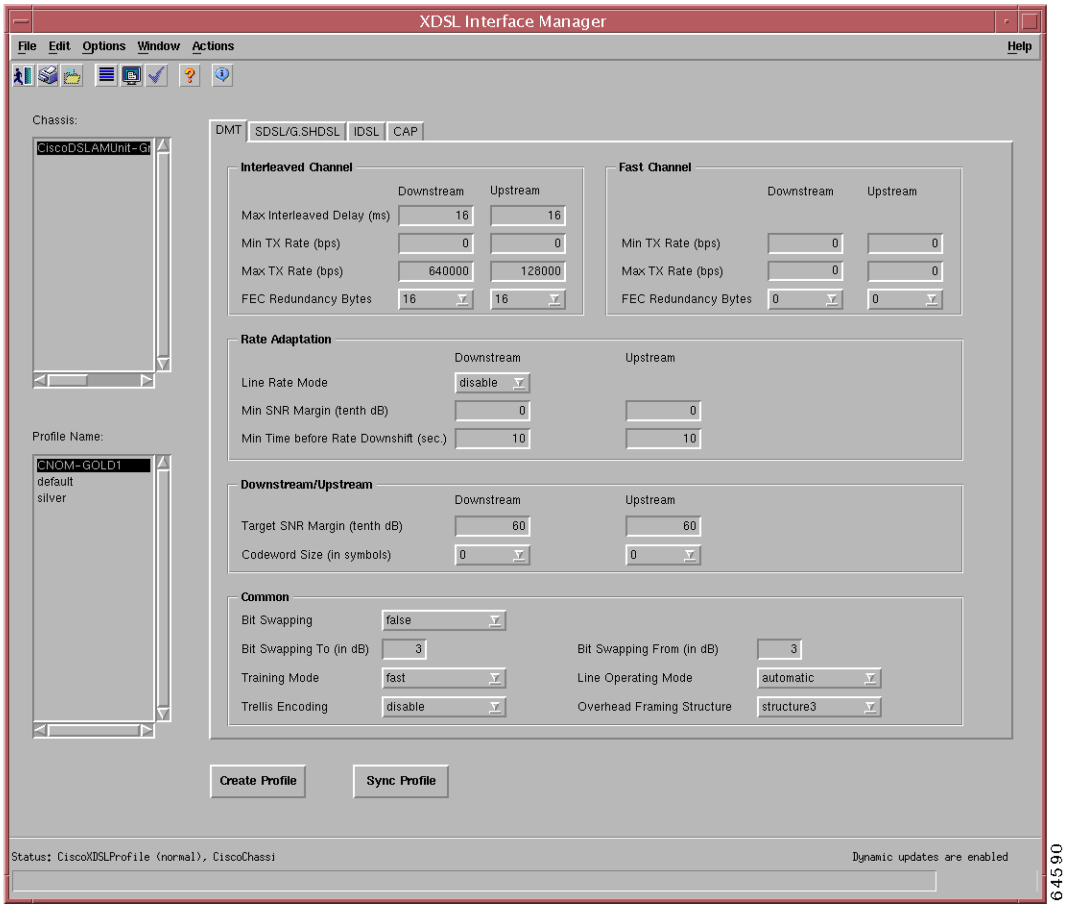
Complete the following steps to create an *x*DSL profile based on an existing profile:

Step 1 Right-click the chassis object for which you want to create a new profile.

Step 2 Choose **Cisco DSL Manager > Chassis > Profile Management > *x*DSL Profiles.**

The XDSL Interface Manager window opens. (See Figure 3-3.)

Figure 3-2 XDSL Interface Manager Window



Step 3 Select the *x*DSL profile you want to use as a model from the profile list box on the left side of the XDSL Interface Manager window.

Step 4 Click **Create Profile**.

Step 5 The Prompt dialog box opens.

Step 6 Enter the new profile name, then click **OK**.

Step 7 Select the newly created profile from the list box on the left.

Step 8 Set the parameters in the DMT tab, the SDSL/G.SHDSL, or the CAP tab for this new *x*DSL profile.

Step 9 Click **Save** to save your changes.

Creating New *x*DSL Profile Parameters

This section includes instructions for creating new *x*DSL profiles and includes the following sections:

- Setting New DMT Parameters, page 3-8
- DMT Tab Field Definitions, page 3-10
- Setting New SDSL/G.SHDSL Parameters, page 3-15
- SDSL/G.SHDSL Tab Field Descriptions, page 3-17
- Setting New CAP Parameters, page 3-18
- CAP Tab Field Definitions, page 3-20

Note The *x*DSL profile IDSL parameters are not applicable to this release of CDM.

To create new *x*DSL profiles, you open the XDSL Interface Manager window, reset the line card parameters as you want them to be, and then create a new profile name for that *x*DSL profile. For example, if you want to create three levels of service and have an *x*DSL profile for each level, you could create Gold, Silver, and Bronze *x*DSL profiles.

In this example, you have DSLAM configurations that include CAP, DMT, and SDSL line cards. To create the Gold level *x*DSL profile, you would

1. Open the XDSL Interface Manager window.
2. Modify the DMT parameter settings for a high-level of service.
3. Modify the SDSL/G.SHDSL parameter settings for a high-level of service.
4. Modify the CAP parameters for a high-level of service.
5. Click the **Create Profile** button and name the profile *Gold*.

You would repeat these steps for the Silver and Bronze *x*DSL profile, setting the parameters appropriately for each level of service. You would then have three new *x*DSL profiles with the names Gold, Silver, and Bronze that you could easily apply to the appropriate subscribers.

Note CDM saves and stores *x*DSL profiles to the IOS configuration on the DSLAM. Only the profile name is stored in CDM.

Note When you modify an *x*DSL profile in CDM and save it with a new name, avoid using spaces in the name of the profile. Your profile name should be compatible with the IOS CLI, which recognizes a space as the end of a profile name. For example, use `newprofiletype` as the name rather than `new profile type`.

Setting New DMT Parameters

This section describes how to set new parameters for DMT line cards and includes the following topics:

- Setting the Interleaved Channel Fields, page 3-13
- Setting the Fast Channel Parameters, page 3-14
- Setting the Rate Adaptation Parameters, page 3-14

- Setting the Downstream/Upstream Parameters, page 3-15
- Setting the Common Parameters, page 3-15

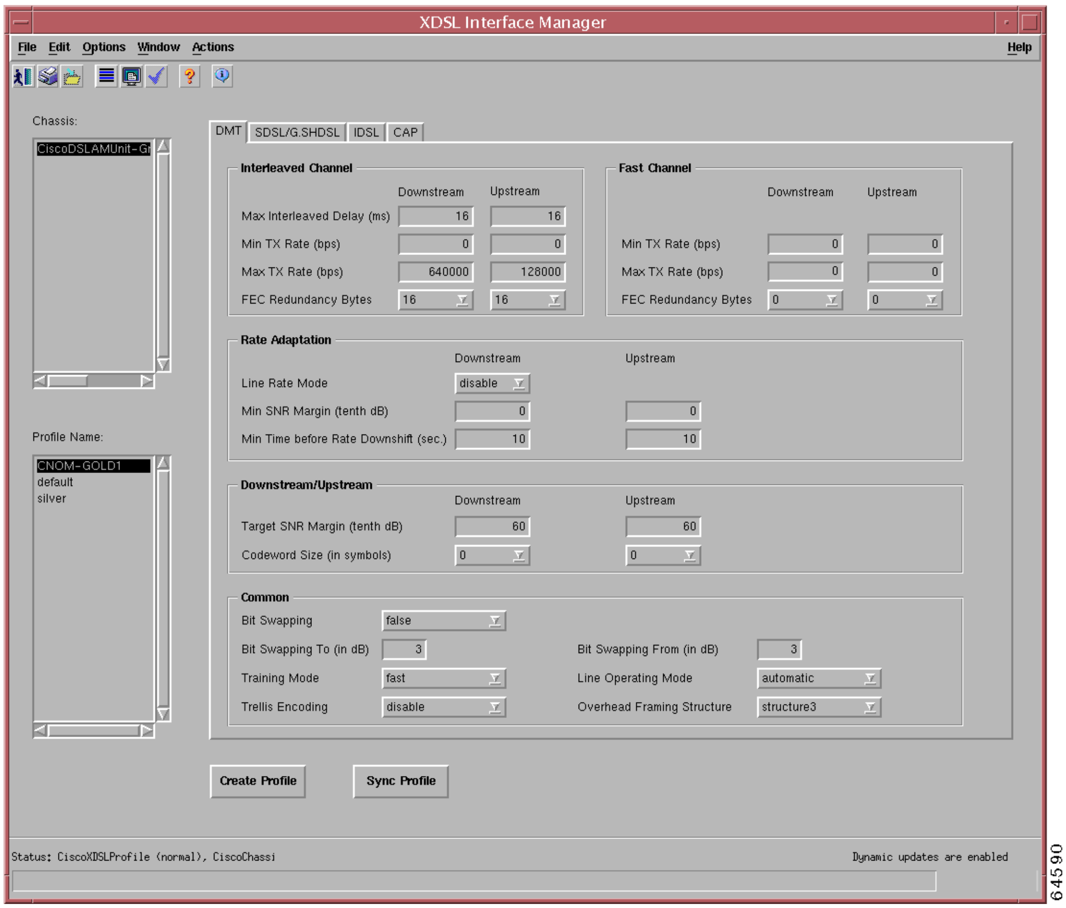
To modify the DMT parameters in the XDSL Interface Manager window, complete the following steps:

Step 1 In the Map Viewer window, within the Component Managed view, right-click the chassis object (DSLAM) for which you want to modify profile parameters to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Profile Management >** ***x*****DSL Profiles.**

The XDSL Interface Manager window opens. (See Figure 3-3.)

Figure 3-3 XDSL Interface Manager Window—DMT Tab



This window opens to the DMT tab. The DMT tab contains five areas:

- Interleaved Channel
- Fast Channel
- Rate Adaptation
- Downstream/Upstream
- Common

Step 3 Click **Create Profile**.

Step 4 Enter the name for the profile in the Prompt dialog box, and then click **OK**.

DMT Tab Field Definitions

The fields in the DMT tab are described in Table 3-2.

Table 3-2 XDSL Interface Manager Window—DMT Tab Field Descriptions

Field	Description
Interleaved Channel	
Max Interleaved Delay (ms)	Sets the number of bytes to be used for interleaved delay. Enter the value for downstream and upstream interleave delay in bytes. This field applies only to the interleave channel and defines the mapping, or relative spacing, that exists (1) between subsequent input bytes at the interleaver input and (2) the placement of the input bytes in the bit stream at the interleaver output.
Min TX Rate (bps)	Specifies the minimum transmit rate. Enter the value for the configured minimum transmit rate for interleave channels in bits per second.
Max TX Rate (bps)	Specifies the maximum transmit rate. Enter the value for the configured maximum transmit rate for interleave channels in bits per second.
FEC Redundancy Bytes	Specifies the initial number of FEC redundancy bytes that the downstream and upstream device frames transmit over the interleaved channel during the training sequence. Valid choices include 0, 2, 4, 6, 8, 10, 12, 14, and 16. The downstream device can fall back from this value depending on the aggregate data rate achieved during training. The value of this object must be an integral multiple of the value displayed in the Codeword Size field.
Fast Channel	
Min TX Rate (bps)	Enter a value from 0 to 8,064,000 in steps of 32,000 to specify the minimum transmit rate for downstream. Enter a value from 0 to 1,024,000 in steps of 32,000 to specify the minimum transmit rate for upstream.
Max TX Rate (bps)	Enter a value from 0 to 8,064,000 in steps of 32,000 to specify the maximum transmit rate for downstream. Enter a value from 0 to 1,024,000 in steps of 32,000 to specify the minimum transmit rate for upstream.
FEC Redundancy Bytes	Enter a value from 0, 2, 4, 6, 8, 10, 12, 14, or 16 to set the initial number of FEC redundancy bytes (downstream and upstream) that the DSLAM appends to the fast channel.

Table 3-2 XDSL Interface Manager Window—DMT Tab Field Descriptions (continued)

Field	Description
Rate Adaptation	
Line Rate Mode	Use the down arrow to choose enable or disable; doing so sets or disables the transmission rate adaptation (downstream only) to adjust the line rate to meet the SNR margin.
Min SNR Margin (tenth dB)	Enter –150 to 150, in increments of 10, to specify the minimum SNR margin in for downstream and upstream.
Min Time before Rate Downshift (sec)	Enter 1 to 60 to specify the minimum time in seconds allowed before the line rate can downshift for downstream and upstream.
Downstream/Upstream	
Target SNR Margin (tenth dB)	Specifies the target SNR margin. Enter the value to set the noise margin that the modem must achieve with a BER of 10^{-7} or better to successfully complete initialization. • If the noise margin is above this level, the modem should attempt to reduce its power output to optimize its operation. • If the noise margin falls below this level, the modem attempts to increase its power output. • If the increase is not possible, the modem attempts to reinitialize or shut down. **Note** Configured allocation ratios of excess transmit bandwidth between fast and interleaved channels apply only when two-channel mode and RADSL are supported.
Codeword Size (in symbols)	Sets the number of symbols per codeword that the downstream and upstream messages use on an interleaved channel during the training sequence. Valid choices include—0, 1, 2, 4, 8, and 16. The downstream can fall back from this value, based on the aggregate data rate achieved during training.
Common	
Bit Swapping	Specifies bit swapping, which can maximize error performance by attempting to maintain an acceptable margin for each bin by equalizing the margin across all bins through bit reallocation.
Bit Swapping To (in dB)	Use the down arrow to choose a number from 0 to 6 as a threshold value. The ATU-C marks a bin as a “to” bin if the bin margin exceeds a specified target value and the difference between the margin and target exceeds a specified threshold value. If this value is too low, the ATU-C might toggle bit allocation on bins frequently. If impulse noise is present, the frequent toggling of bit allocation can cause errors. If this value is too high, the ATU-C might not identify an adequate number of bins to which it can swap bits, which reduces the ability of the ATU-C to equalize the margin across all bins.

Table 3-2 XDSL Interface Manager Window—DMT Tab Field Descriptions (continued)

Field	Description
Training Mode	Use the down arrow to choose standard of fast to set the mode that the downstream and upstream devices use when the devices are training against each other. The default training mode for ADSL modems is standard.
Trellis Encoding	Use the down arrow to set enabled or disable. Trellis coding is a method of forward error correction in which each signal is assigned a coded binary value. This value represents the phase and amplitude of that signal, allowing the receiving modem to determine whether a given signal is received in error.
Bit Swapping From (in dB)	Use the down arrow to choose 0 to 6 as a threshold value. The ATU-C marks a bin as a "from" bin if the bin margin falls below a specified target value, and the difference between the margin and target exceeds a specified threshold value. If you set this value too low, the ATU-C may frequently toggle the bit allocation on bins. If impulse noise is present, the frequent toggling of bit allocation can cause errors. If you set this value too high, the ATU-C may not identify an adequate number of bins from which it can swap bits. This situation decreases the ability of the ATU-C to equalize the margin across all bins.

Table 3-2 XDSL Interface Manager Window—DMT Tab Field Descriptions (continued)

Field	Description
Line Operating Mode	Use the down arrow to select from the following operating modes: • automatic—In this mode, the ATU-C automatically detects the capabilities of the ATU-R CPE and uses a startup sequence that is specified by G.992.1, G.992.2, or T1.413-1998. The default for an ADSL line is auto mode. • g992Dot1—In this mode, the ATU-C requests the G994.1 startup sequence. After startup, the line complies to G992.1 operation. This mode is used in European configurations (Annex B). • g992Dot2—In this mode, the ATU-C requests the G994.1 startup sequence. After startup, the line complies to G992.2 operation. G992.2 is also known as G.lite. This mode is used in European configurations (Annex B). • t1Dot413—In this mode, the ATU-C requests the T1.413-1998 startup sequence. After startup, the line complies to T1.41-1998 operation.
Overhead Framing Structure	Use the down arrow to set the negotiated overhead framing structure that the downstream device and upstream device use. Choose from among the following modes: • 0 = Full Asynchronous. Full-overhead framing with asynchronous bit-to-modem timing (enabled synchronization control mechanism). • 1 = Full Synchronous. Full-overhead framing that uses synchronous bit-to-modem timing, a disabled synchronization control mechanism. • 2 = Reduced Separate Fast. Reduced-overhead framing that has separate fast and sync bytes. Bytes exist in fast and interleaved latency buffer respectively (64 kbps framing overhead). • 3 = Reduced Merged Fast. Reduced overhead framing with merged fast and dsync byte, using either the fast or interleaved latency buffer (32 kbps framing overhead). This is the recommended setting. **Note** G.lite line rates allow only for an overhead frame value of 3.

Setting the Interleaved Channel Fields

The DMT interface can be set to either interleaved or fast; the choices are mutually exclusive. The default setting is interleaved. Therefore, if you want to set the DMT interface to fast, you must enter zeros (0s) in all of the interleaved Channel area fields in the DMT tab.

Complete the following steps to set the interleaved channel fields. Use the GUI tooltips as a guide to the available valid values. Also see Table 3-2.

Step 1 Enter the appropriate variable in the Max Interleaved Delay (ms) field to set the interleave delay for both downstream and upstream.

If you are setting the Fast Channel parameters instead, enter 0 for both Downstream and Upstream in this field.

Note You must set the fields in the Interleaved Channel area to 0 if you want to set the Fast Channel fields for a DMT card. If you allow values to remain in these field, CDM issues an error.

Step 2 Enter the appropriate variable in the Max TX Rate (bps) field for both Downstream and Upstream.

If you are setting the Fast Channel parameters instead, enter 0 for both Downstream and Upstream in this field.

Step 3 Enter the appropriate variable in the Min TX Rate (bps) field for both Downstream and Upstream.

If you are setting the Fast Channel parameters instead, enter 0 for both Downstream and Upstream in this field.

Step 4 Use the down arrow to select the appropriate value in the FEC Redundancy Bytes field for both Downstream and Upstream.

If you are setting the Fast Channel parameters instead, enter 0 for both Downstream and Upstream in this field.

Setting the Fast Channel Parameters

Complete these steps to set the fast channel fields. Remember to set the all of the fields in the Interleaved Channel area to 0 if you are setting Fast Channel parameters. Use the GUI tooltips as a guide to the available valid values. Also see Table 3-2.

Step 1 Enter the appropriate variable in the Max TX Rate (bps) field for both Downstream and Upstream.

Step 2 Enter the appropriate variable in the Min TX Rate (bps) field for both Downstream and Upstream.

Step 3 Use the down arrow to select the appropriate value in the FEC Redundancy Bytes field for both Downstream and Upstream.

Setting the Rate Adaptation Parameters

Complete these steps to set the fields in the Rate Adaptation area in the DMT tab. Use the GUI tooltips as a guide to the available valid values. Also see Table 3-2.

Step 1 Use the down arrow to select **Enable** or **Disable** in the Line Rate Mode field.

Step 2 Enter the appropriate value in the Min SNR Margin (tenth dB) field.

Step 3 Enter the appropriate value in the Min Time before Rate Downshift (sec) field.

Setting the Downstream/Upstream Parameters

Complete these steps to set the common fields. Use the GUI tooltips as a guide to the available valid values. Also see Table 3-2.

Step 1 Enter the value for Target SNR Margin (in tenth dB) for both Downstream and Upstream.

Step 2 Use the down arrow to select the codeword in the Codeword Size (in symbols) field.

Setting the Common Parameters

Complete these steps to set the common fields. Use the GUI tooltips as a guide to the available valid values. Also see Table 3-2.

Step 1 In the Bit Swap field, use the down arrow to select **true** or **false** to set or turn off bit swapping.

Step 2 In the Bit Swap Margin To (in dB) field, enter an appropriate value from the range of 1 to 9.

Step 3 In the Bit Swap Margin From (in dB) field, enter an appropriate value from the range of 1 to 9.

Step 4 In the Training Mode field, use the down arrow to select fast or standard training.

Step 5 In the Line Operating Mode field, use the down arrow to select which line-operating mode the ADSL line will use.

Step 6 In the Trellis Encoding field, use the down arrow to select **enable** or **disable** to set whether trellis coding is used on the DMT line.

Step 7 In the Overhead Framing field, use the down arrow to set the negotiated overhead framing structure that the downstream device and upstream device use.

Step 8 Click the **Save** icon or choose **File > Save** from the menu bar.

CDM creates, saves, and stores the newly defined profile.

Setting New SDSL/G.SHDSL Parameters

You can set *x*DSL profile SDSL/G.SHDSL parameters to apply to SDSL or G.SHDSL interfaces. One set of SDSL or G.SHDSL parameters can be applied to multiple SDSL or G.SHDSL interfaces on a card.

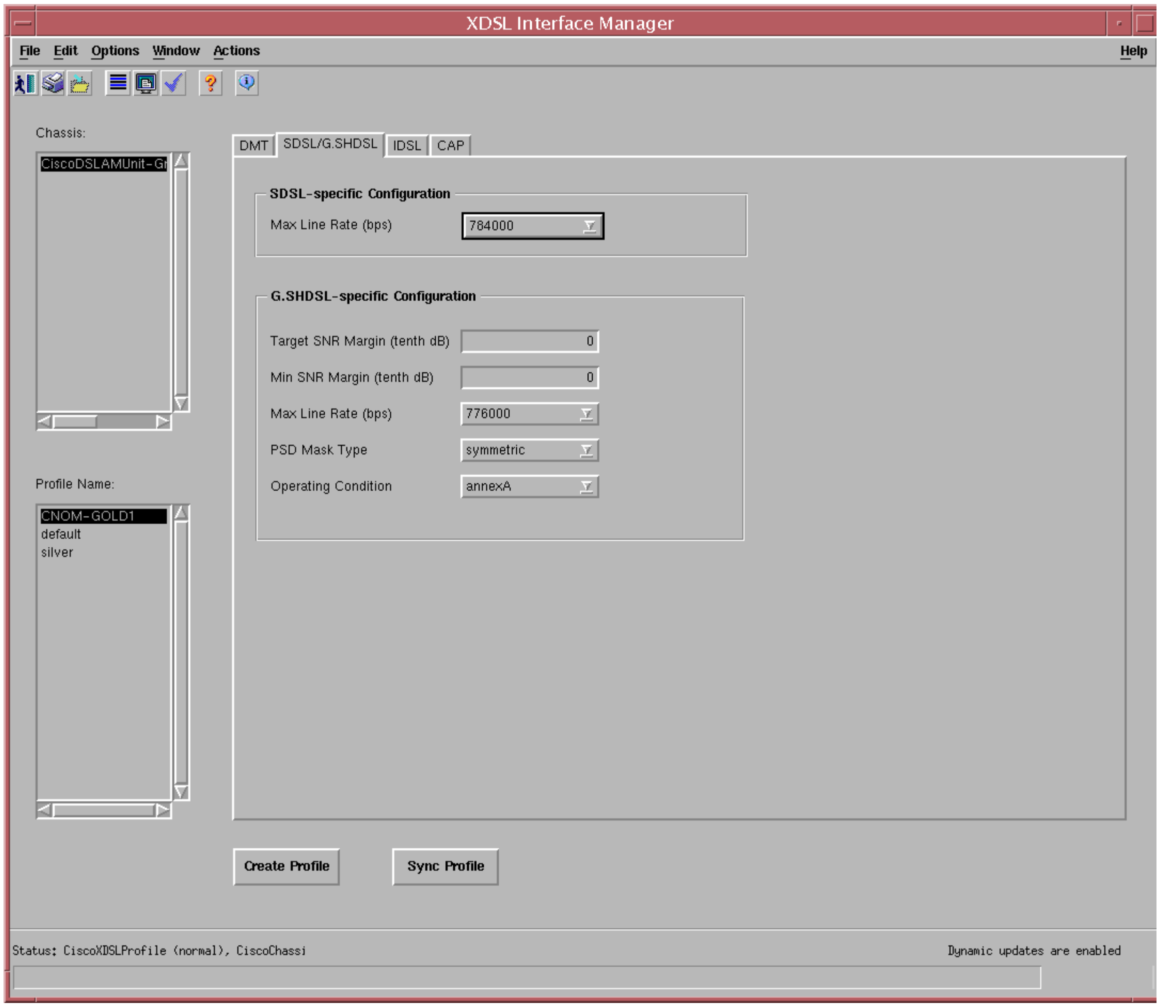
To modify *x*DSL profile SDSL or G.SHDSL parameters for an SDSL interface, complete the following steps:

Step 1 In the Map Viewer window, within the Component Managed view, right-click the chassis object (DSLAM) for which you want to modify profiles to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Profile Management > *x*DSL Profiles**.

Step 3 Click the **SDSL/G.SHDSL** tab, (see Figure 3-4).

Figure 3-4 XDSL Interface Manager Window—SDSL/G.SHDSL Tab



The SDSL/G.SHDSL tab contains two areas—SDSL-specific Configuration and G.SHDSL-specific Configuration.

Step 4 Select the profile that you want to use as a template from the list box on the left.

Step 5 Click **Create Profile**.

Step 6 Enter the name for the new profile in the Prompt dialog box, and then click **OK**.

Step 7 Use the GUI tooltips and refer to Table 3-3 to set the fields in this tab as follows:

a. In the SDSL-specific Configuration area, use the down arrow in the Max Line Rate (bps) field to select the maximum bit rate you want to set for the SDSL profile.

The remaining fields are in the G.SHDSL-specific Configuration area. Enter these values in multiples of 10.

b. In the Target SNR Margin (tenth dB) field, enter the value for the target signal-to-noise ratio margin.

c. In the Min SNR Margin (tenth dB) field, enter the setting for the minimum SNR margin.

d. In the Max Line Rate (bps) field, use the down area to select the maximum line rate for the G.SHDSL profile.

e. In the SHDSL PSD masktype field, use the down arrow to select **symmetric**.

   This object specifies the PSD mask type for the transceiver. For all values of the SHDSL bit rate field, you can select the symmetric PSD mask type.

f. In the Operating Condition field, use the down arrow to select Annex A or Annex B.

Step 8 Click the **Save** icon or choose **File > Save** to save your changes.

SDSL/G.SHDSL Tab Field Descriptions

The fields in the SDSL/G.SHDSL tab are described in Table 3-3.

Table 3-3 SDSL/G.SHDSL Tab Field Descriptions

Field	Description
SDSL-Specific Configuration	
(SDSL) Max Line Rate (bps)	Specifies the SDSL maximum line rate from the following choices (in bits per second): • 144000 • 272000 • 400000 • 528000 • 784000 • 1040000 • 1168000
G.SHDSL-Specific Configuration	
Target SNR Margin (tenth dB)	Specifies the noise margin that the STU-C must achieve with a BER of 10^{-7} or better to successfully complete training. Valid values are 0 to 31 dB.
Min SNR Margin (tenth dB)	Specifies the minimum acceptable SNR margin. If the noise margin falls below this level, the STU-C retrains. Valid values are 0 to 31 dB.

Table 3-3 SDSL/G.SHDSL Tab Field Descriptions (continued)

Field	Description
(G.SHDSL) Max Line Rate (bps)	Specifies the maximum G.SHDSL line rate from the following choices: • 72000 • 136000 • 200000 • 264000 • 392000 • 520000 • 776000 • 1032000 • 1160000 • 1544000 • 2056000 • 2312000
PSD Mask Type	Use the down arrow to choose symmetric or asymmetric. This field specifies the PSD mask type for the transceiver. For all values of the SHDSL bit rate field, you can select the symmetric PSD mask type. Asymmetric supports 776000, 784000, 1552000, 205600000, 2312000, which are the maximum line rates to which the asymmetric PDS mask type can apply.
Operating Condition	Select either Annex A or Annex B in this field. • Annex A is optimized for conditions that are typically encountered within the North American network. • Annex B is optimized for conditions that are typically encountered within the European network.

Setting New CAP Parameters

You can modify *x*DSL profile CAP parameters to apply to flexi CAP interfaces. One set of CAP parameters can be applied to multiple flexi CAP interfaces on a card.

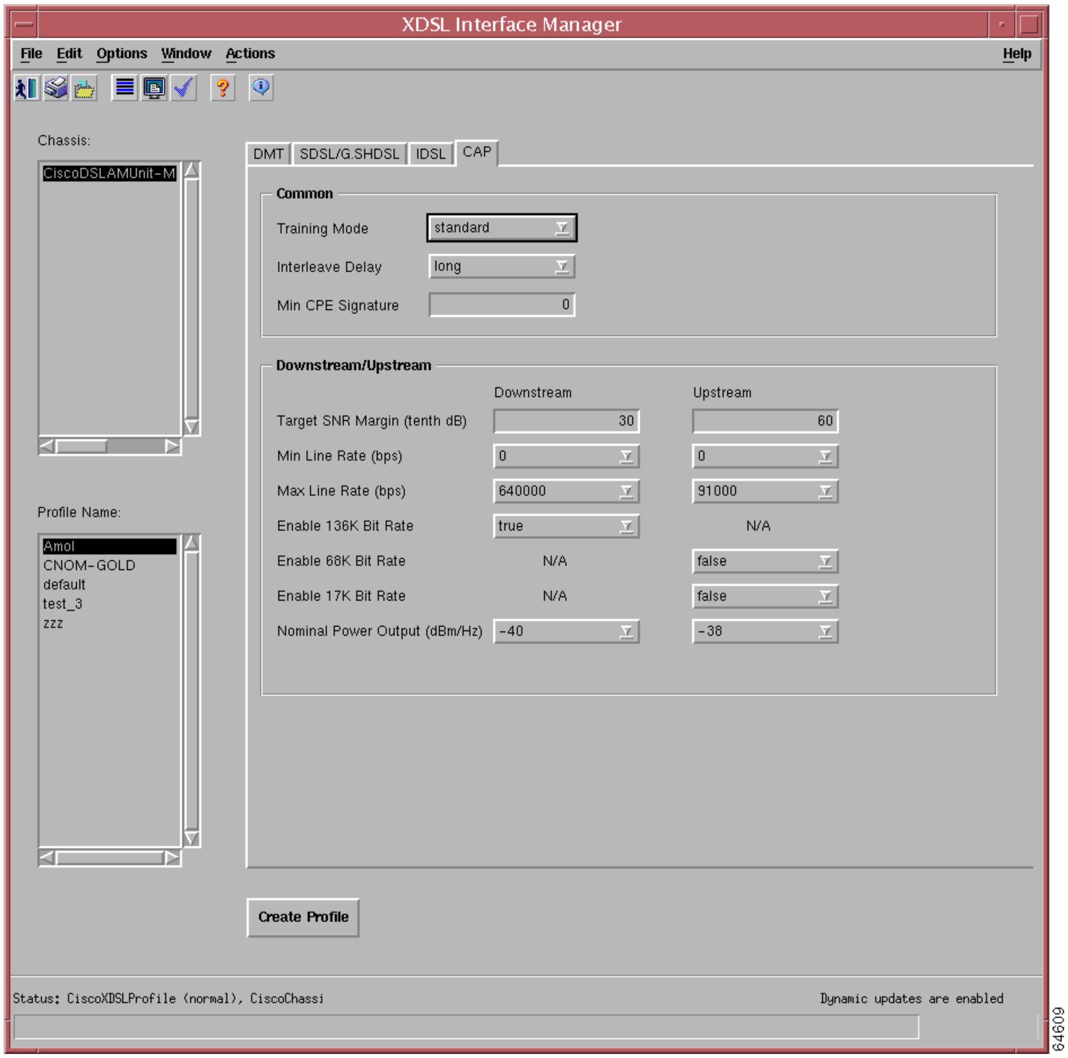
To modify CAP profile parameters, complete the following steps:

Step 1 In the Map Viewer window, within the Component Managed view, right-click the chassis object (DSLAM) for which you want to manage profiles to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Profile Management > *x*DSL Profiles.**

The XDSL Interface Manager window opens. (See Figure 3-5.)

Figure 3-5 XDSL Interface Manager Window—CAP Tab



Step 3 Click the **CAP** tab.

The CAP tab contains two areas—Common and Downstream/Upstream.

Step 4 Click **Create Profile**.

The Prompt dialog box opens.

Step 5 Enter the new profile name and click **OK**.

See Table 3-4 and use the GUI tooltips to set the parameters on the CAP tab.

Step 6 In the Common area, set the following parameters:

a. Use the down arrow in the Training Mode field to set this to Standard.

b. Use the down arrow in the Interleave Delay field to set this field to none, short, or long.

c. Enter the appropriate value in the Min CPE Signature field.

Step 7 In the Downstream/Upstream area, set the following parameters:

a. Enter the appropriate values in the Target SNR Margin (tenth dB) for both downstream and upstream.
b. Use the down arrow to set the Min Line Rate (bps) field for both downstream and upstream.
c. Use the down arrow to set the Max Line Rate (bps) field for both downstream and upstream.
d. Use the down arrow to set the Enable 136K Bit Rate (bps) field to true or false, downstream only.
e. Use the down arrow to set the Enable 68K Bit Rate (bps) field to true or false, upstream only.
f. Use the down arrow to set the Enable 136K Bit Rate (bps) field to true or false, upstream only.
g. Use the down arrow to set the Nominal Power Output (dBm/Hz) (bps) field for both downstream and upstream.

Step 8 Click the **Save** icon or choose **File > Save** to save your changes.

Note See Table 3-4 for descriptions of the fields on the CAP tab.

CAP Tab Field Definitions

The CAP tab has two areas—Common and Downstream/Upstream. Table 3-4 describes the CAP tab fields.

Table 3-4 CAP Interface Profile Window Field Definitions

Field	Description
Common	
Training Mode	Use the down arrow to select Standard or Fast; currently the only mode supported by Cisco IOS is standard.
Interleave Delay (milliseconds)	Use the down arrow to choose the delay for interleave in milliseconds. Valid values are none, short, and long interleave. Choose short for time-sensitive traffic; choose long for time-insensitive traffic. This field sets the relative spacing between input bytes at the interleaver input for the line.
Min CPE[1] Signature	Enter the number that represents the type of CPE that connects to the DSLAM chassis from 0 to 127.

Table 3-4 CAP Interface Profile Window Field Definitions (continued)

Field	Description
Downstream/Upstream	
Target SNR[2] Margin (tenth dB)	Enter from 0 to 310 to specify the noise margin that the modem must achieve with a BER[3] of 10^{-7} or better to successfully complete initialization. If the noise margin is above this level, the modem should attempt to reduce its power output to optimize operation. If the noise margin falls below this level, the modem should attempt to increase its power output. If the modem is unable to increase its power output, it attempts to reinitialize or shut down. **Note** Configured allocation ratios of excess transmit bandwidth between fast and interleaved channels only apply when two-channel mode and RADSL[4] are supported.
Min Line Rate (bps)	Use the down arrow to select the minimum bit rate recommended for this profile from among the following choices in bps—0, 256000, 384000, 512000, 640000, 768000, 896000, 960000, 1024000, 128000, 1600000, 1920000, 2240000, 2560000, 2688000, 3200000, 4480000, 5120000, 6272000, or 7168000.
Max Line Rate (bps)	Use the down arrow to select the maximum recommended bit rate for this profile from among the following choices in bps—0, 91000, 272000, 408000, 544000, 680000, 816000, 952000, or 1088000.
Enable 136 K Bit Rate	Use the down arrow to select true or false for CAP cards that support 136 kilobaud training rates; downstream only.
Enable 68 K Baud	Use the down arrow to set to true or false. CAP cards support 68 kilobaud training rates; upstream only.
Enable 17 K Bit Rate	Use the down arrow to set to true or false. CAP cards support 17 kilobaud training rates; upstream only.
Nominal Power Output (dBm/Hz)	Use the down arrow to set the transmit power in dBm/Hz from the following choices: • Downstream: –17, –40, –43, –46, –49, –52 • Upstream: –38, –41, –44, –47, –50, –53

1. CPE = customer premises equipment
2. SNR = signal to noise ratio
3. BER = bit error rate
4. RADSL = rate adaptive digital subscriber line

Deleting an *x*DSL Profile

To delete an existing *x*DSL profile, complete these steps. You can delete a profile only if it is not currently in use.

Step 1 From the Component Managed view, right-click the *x*DSL profile that you to delete.

Or, open the XDSL Interface Manager window and choose the profile from the list box that you want to delete and right-click.

Note You can also hold down the shift key to select more than one profile.

Step 2 Choose **Deployment > Delete Objects** from the object menu

The Deployment Wizard Summary window opens.

Step 3 Click **Finish** to delete the selected profile.

A message displays in the Deployment Wizard Summary window to confirm successful deletion.

You cannot delete a profile that is currently in use. If you want to view the subscribers that are using a specific profile, you can run a Cisco EMF query against the profile name. (Refer to the *Cisco Element Management Framework User Guide* for details about how to run a query.)

Tip Here is a workaround for removing an applied *x*DSL profile from an interface or module port through the CDM GUI. Apply a default or another profile to the interface whose applied profile is the one that you want to delete. After CDM overwrites the applied profile with either the default profile or a different profile, you can delete the previously applied profile.

Viewing and Applying *x*DSL Profiles

This section includes instructions for viewing and applying *x*DSL profiles and includes the following topics:

- Viewing xDSL Profiles, page 3-22
- Applying xDSL Profiles, page 3-24

Viewing *x*DSL Profiles

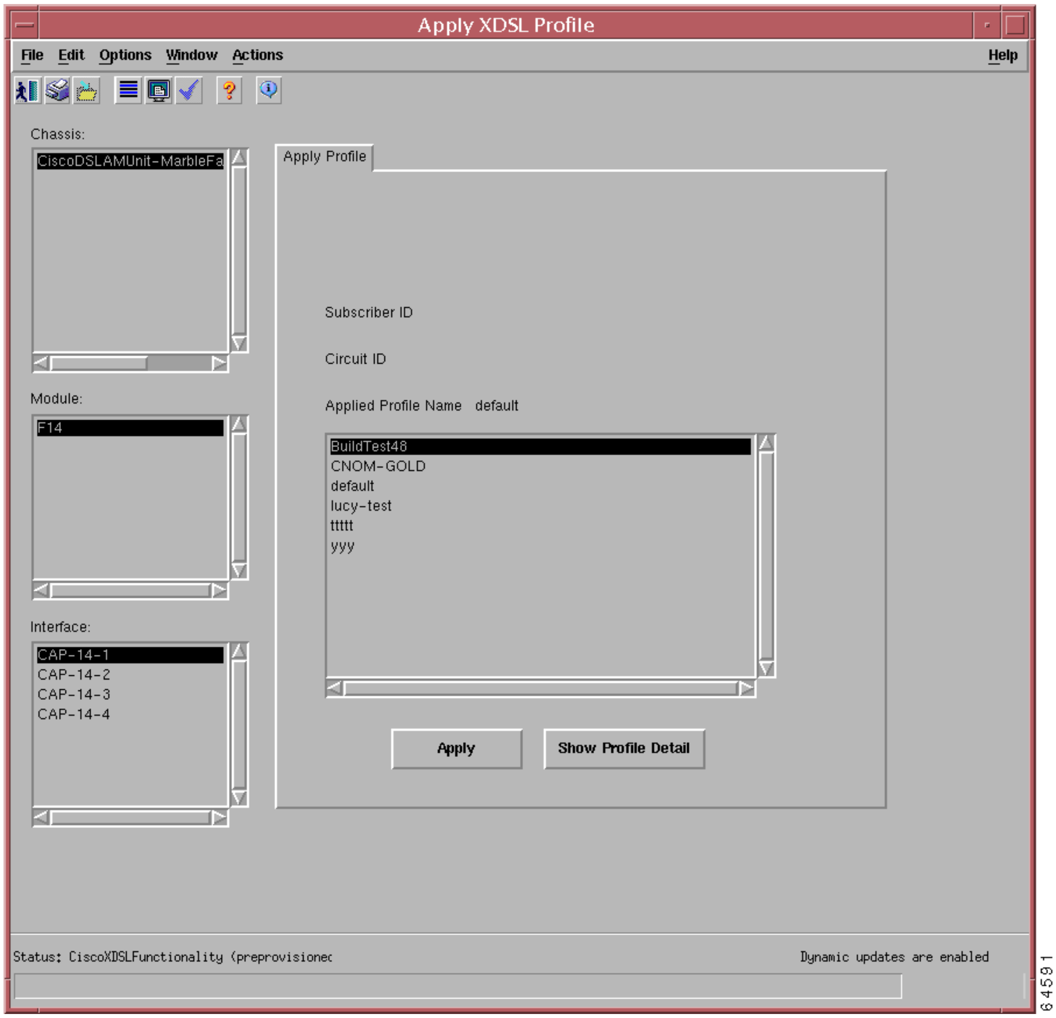
Complete the following steps to view the details of any *x*DSL profile:

Step 1 Within the Component Managed view, right-click the interface whose profile description you want to view.

Step 2 Choose Cisco **DSL Manager > Interface > Configuration > *x*DSL** from the object menu.

The Apply XDSL Profile window opens. (See Figure 3-6.)

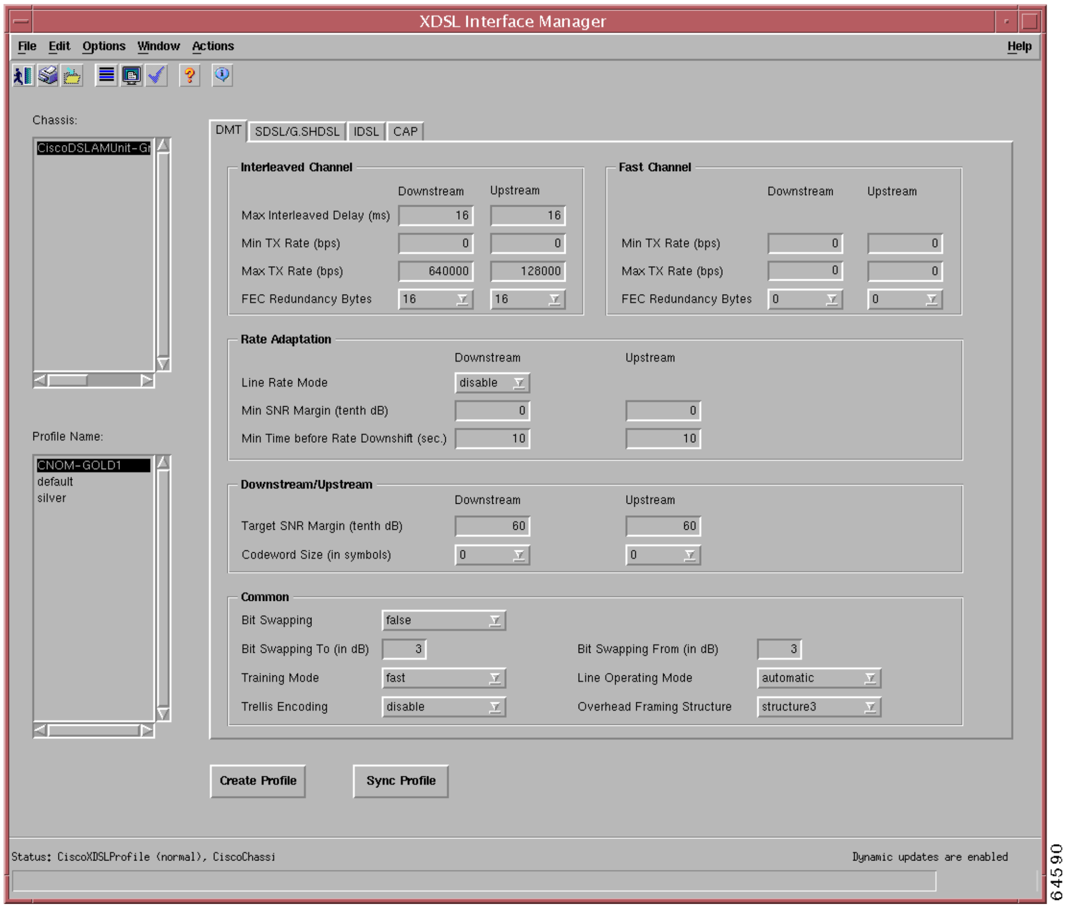
Figure 3-6 Apply XDSL Profile Window



Step 3 Click **Show Profile Detail**.

The XDSL Interface Manager window opens, in which you can view the details of this profile. (See Figure 3-7.)

Figure 3-7 XDSL Interface Manager Window



Step 4 Click the **Close** icon to close the XDSL Interface Manager window.

Applying *x*DSL Profiles

You can apply profiles to an interface only if the module and interface are in normal, preprovisioned, performance logging on, or errored state. If the module or interface is in lostcomms, decommissioned, or commissioning state, CDM will issue a failure when you attempt to apply profiles.

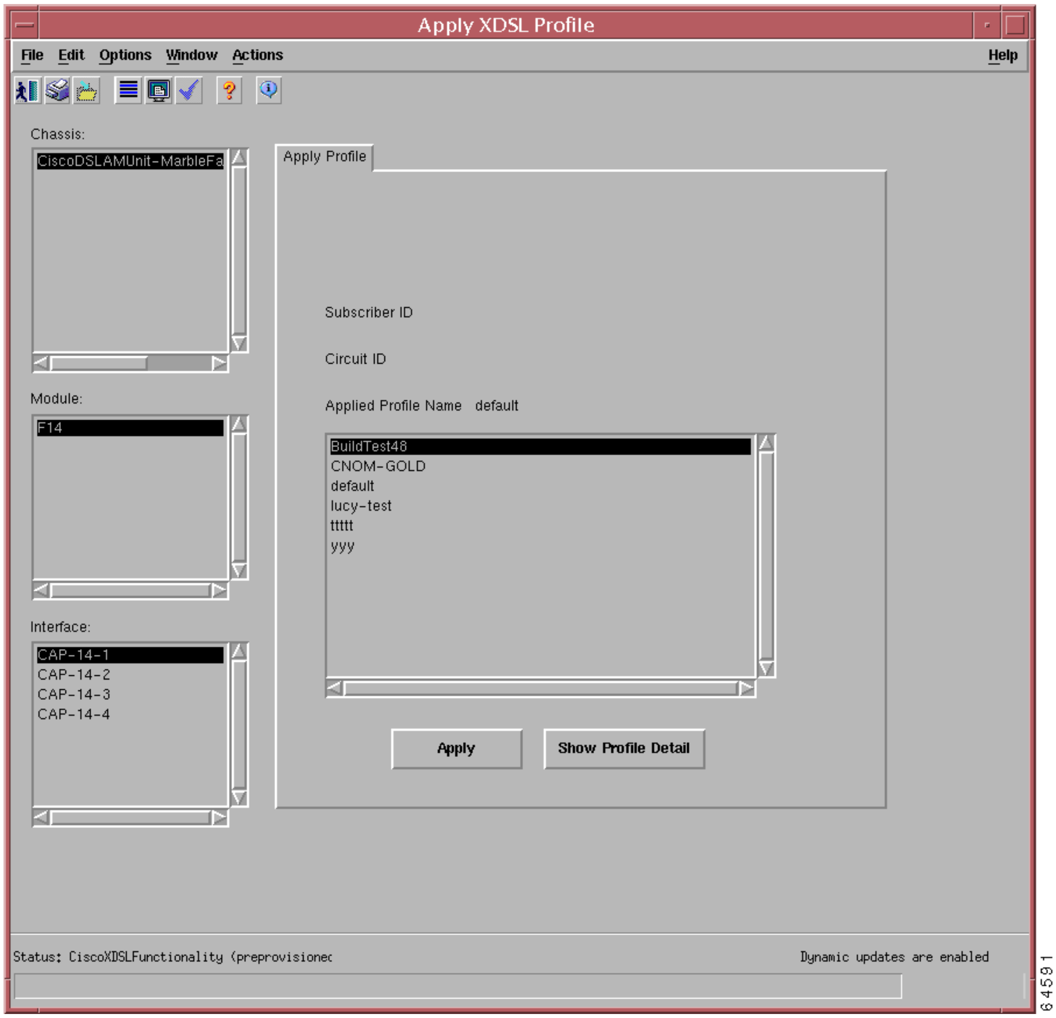
Complete the following steps to apply profiles:

Step 1 Within the Component Managed view, right-click the interface whose profile description you want to view.

Step 2 Choose Cisco **DSL Manager > Interface > Configuration >** ***x*****DSL** from the object menu.

The Apply XDSL Profile window opens. (See Figure 3-8.)

Figure 3-8 Apply XDSL Profile Window



Step 3 In the Applied Profile Name list in the Apply XDSL Profile window, click the *x*DSL profile you want to apply; this highlights the profile.

Step 4 Click the interface to which you want to apply this profile from the list box in the Interface area on the left side of the Apply XDSL Profile window.

You can use the shift key to select more than one interface.

Step 5 Click **Apply** to apply this profile.

Creating Connections and ATM QoS Profiles

This chapter describes how to use the connection synchronization policy feature, how to create PVCs and SPVCs, how to manage virtual channels links (VCLs), how to manually upload ATM connections and create ATM quality of service (QoS) profiles, and how to use inverse multiplexing over ATM (IMA) on Cisco 6015 and 6160 DSLAMs.

This chapter includes the following sections:

Polling the Chassis and Setting the Connection Synchronization Policy

This section describes two features that preserve the synchronization of CDM and DSLAM configurations after you deploy and commission the DSLAM through CDM. This section includes the following topics:

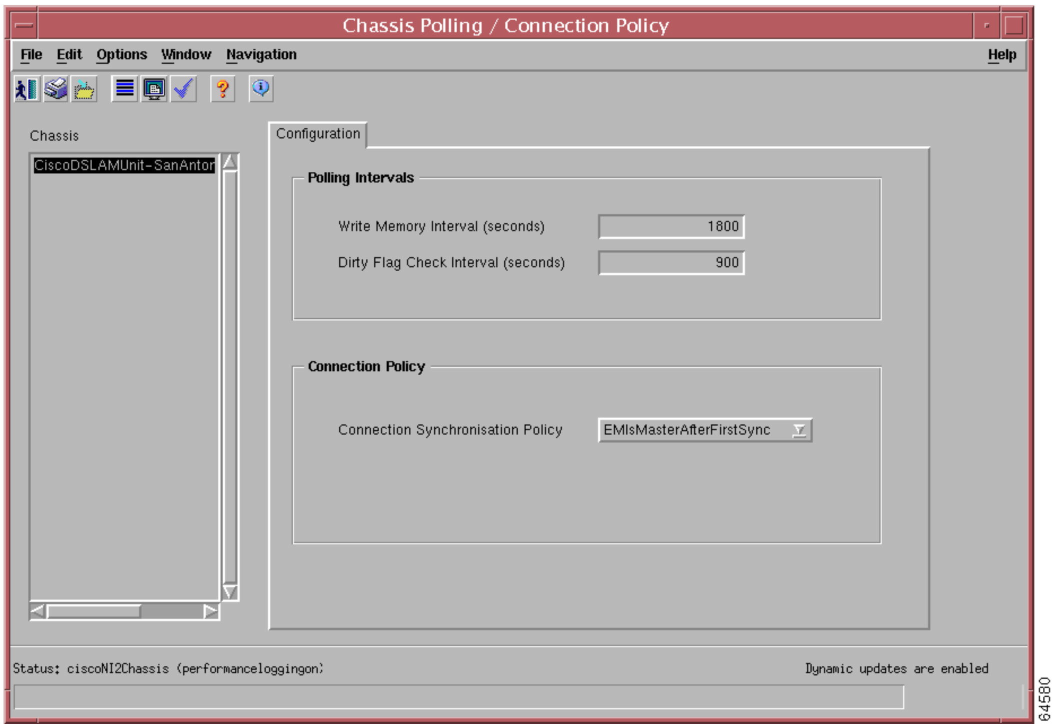
These two features, which you can set in the Chassis Polling/Connection Policy window, include:

- Chassis Polling—Automatically saves configuration data from the DSLAM running configuration to the DSLAM startup configuration.
- Connection Synchronization Policy—Configures the synchronization of PVC or SPVC data between CDM and the DSLAM. If you do not choose to set policy, a default policy is set.

CDM automatically synchronizes connection information, that is, PVCs and SPVCs, between the DSLAM and CDM. In certain cases when you make a change to the IOS running configuration, such as creating or deleting a PVC, CDM might not save the change to the startup configuration before the DSLAM reboots. In this case, you can set three policies to specify how the data is synchronized. These are described in the "Overview of the Connection Synchronization Policy" section on page 4-5.

The Chassis Polling/Connection Policy window is shown in Figure 4-1.

Figure 4-1 Chassis Polling/Connection Policy Window



Overview of Chassis Polling

The chassis polling feature instructs CDM to periodically poll the DSLAM for changes to the running configuration. If the polling process determines that the running configuration has changed, CDM sets an internal flag, called a dirty flag, against the DSLAM. The value that you set in the Dirty Flag Check Interval field in the Chassis Polling/Connection Policy window determines the polling interval (in seconds), as shown in Figure 4-1.

CDM periodically polls the value of the dirty flag. If CDM sets the dirty flag to TRUE, CDM saves the running configuration in the chassis. CDM writes the running configuration into the startup configuration only if the internal dirty flag is TRUE. This operation is referred as the *write mem* operation. You can define how often CDM performs the write mem operation in the Write Memory Interval field in the Chassis Polling/Connection Policy window. The default value for the Write Memory Interval is 1800 seconds; the value range is from 1800 to 86400 seconds.

Setting Polling Intervals

When changes occur on the DSLAM, the polling function checks the running configuration against the saved configuration. If a change has occurred, and the device has not saved the configuration, CDM issues a dirty flag.

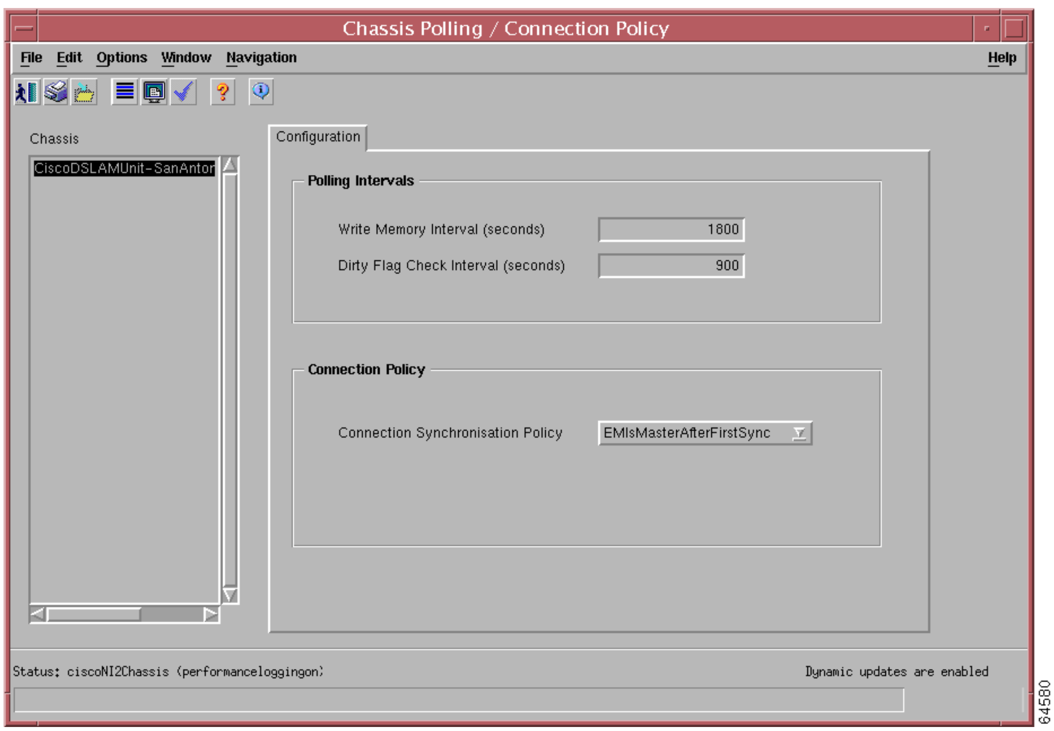
You can set the polling interval and the dirty flag check interval in the Chassis Polling/Connection Policy window as follows.

Step 1 On the Map Viewer window, within the Physical view, click the chassis object whose connection policy you want to set.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > Chassis Polling/Connection Policy** from the object menu.

The Chassis Polling/Connection Policy window opens. (See Figure 4-5.)

Figure 4-2 Chassis Polling/Connection Policy Window



The area for setting intervals is the Polling Intervals area.

Step 3 In the Write Memory Interval (seconds) field, enter the number of seconds to specify how often you want CDM to perform a write memory (and save the configuration).

The default setting is 1800 seconds.

Step 4 In the Dirty Flag Check Interval (seconds), enter the number of seconds to specify how often you want CDM to check for a dirty flag.

The default setting is 900 seconds.

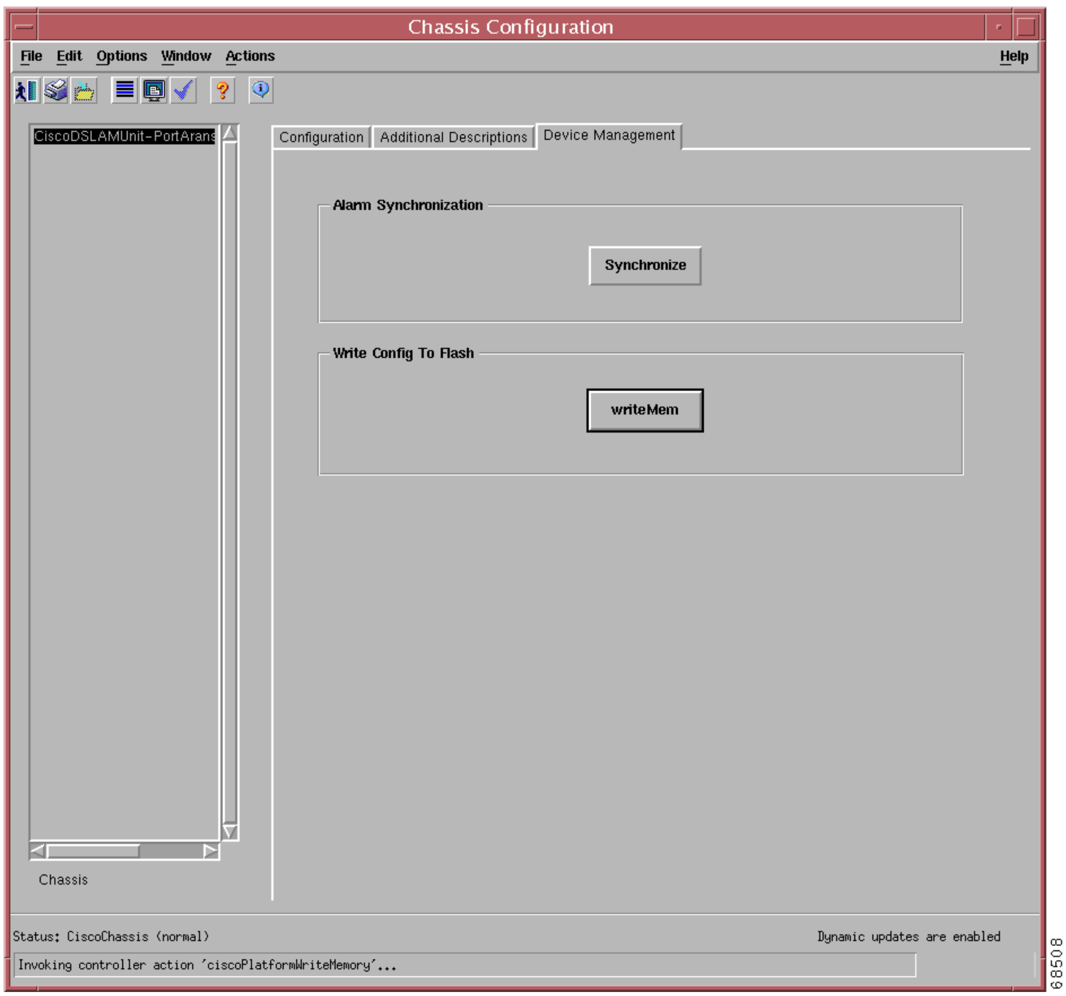
CDM checks the running configuration against the saved configuration to see whether a change has occurred on the DSLAM since the last configuration save. If a change has occurred, CDM sets the dirty flag (marked "dirty"). The next time the writemem task executes, it checks the state of the dirty flag. If CDM sets the dirty flag, the writemem task writes the IOS running configuration to the startup configuration.

Step 5 Click the **Save** icon in the toolbar to save the settings.

Synchronizing Alarms and Saving the Running Configuration

You can save the DSLAM running configuration in the Chassis Configuration window, which opens to the Device Management tab. (See Figure 4-3.)

Figure 4-3 Chassis Configuration Window—Device Management Tab

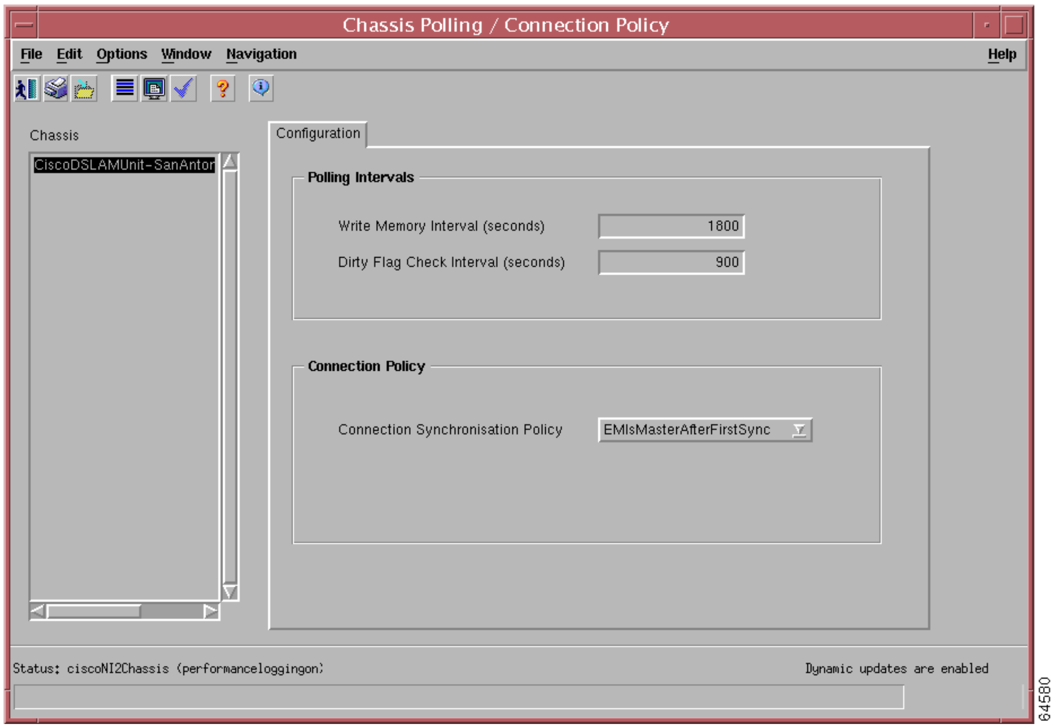


Click the **writeMem** button to force a write memory operation on a selected chassis and save the DSLAM IOS running configuration to the startup configuration.

Overview of the Connection Synchronization Policy

You can set policy (rules) to instruct CDM to automatically synchronize PVCs and SPVCs, between CDM and the DSLAM. You set this parameter in the in the Connection Policy area of the Chassis Polling/Connection Policy window. (See Figure 4-4.)

Figure 4-4 Chassis Polling/Connection Policy Window



The value that you select in the Connection Synchronization Policy field also determines which PVC and SPVC ATM connections CDM will upload when you use the ATM Connection Upload window to upload ATM connections.

The three types of synchronization policies include:

- **Normal**—No action. The DSLAM is master, but do not add a connection to or delete a connection from CDM.
- **DeviceisMaster**—The default. This setting specifies that the DSLAM (device) is the reference point for PVC creations and deletions. CDM will sync up to the device. If a connection is present on the DSLAM but not in CDM, CDM will create the connection. If a connection is absent on the DSLAM but present in CDM, CDM will delete the connection.
- **EMIsMasterAfterFirstSync**—This setting specifies that the element manager, that is, CDM, is the reference point for PVC creations and deletions. The device syncs up to CDM for information about PVC settings. If the connection is present in CDM but not the DSLAM, CDM creates the connection in the DSLAM. If the connection is absent in CDM but present in the DSLAM, CDM deletes the connection from the DSLAM.

The default policy is DeviceisMaster. When you deploy and commission a DSLAM, CDM first copies the device IOS information into CDM. After commissioning is complete, CDM becomes the reference point for PVC creations and deletions.

Table 4-1, Table 4-2, and Table 4-3 describe the behaviors associated with the settings of the synchronization policies.

Table 4-1 Connection Policy—Normal

Connection in CEMF	Connection State in CEMF	Connection State in DSLAM	Synchronization Policy Behavior
Present	Normal	Not present	Change state to decommission.
Present	Decommission	Not present	Do not do anything.
Present	Normal	Present	No action needed.
Present	Decommission	Present	Change state to normal.
Not present	—	Present	Create in CEMF.

Table 4-2 Connection Policy—Device is Master

Connection in CEMF	Connection State in CEMF	Connection State in DSLAM	Synchronization Policy Behavior
Present	Normal	Not present	Remove from CEMF.
Present	Decommission	Not present	Remove from CEMF.
Present	Normal	Present	No action needed.
Present	Decommission	Present	Change cemf state to normal.
Not present	—	Present	Create in CEMF.

Table 4-3 Connection Policy—CEMF is Master After First Sync

Connection in CEMF	Connection State in CEMF	Connection State in DSLAM	Synchronization Policy Behavior
Present	Normal	Not present	Create in device.
Present	Decommission	Not present	No action needed.
Present	Normal	Present	No action needed.
Present	Decommission	Present	Remove from device.
Not present	—	Present	Remove from device.

Setting the Connection Synchronization Policy

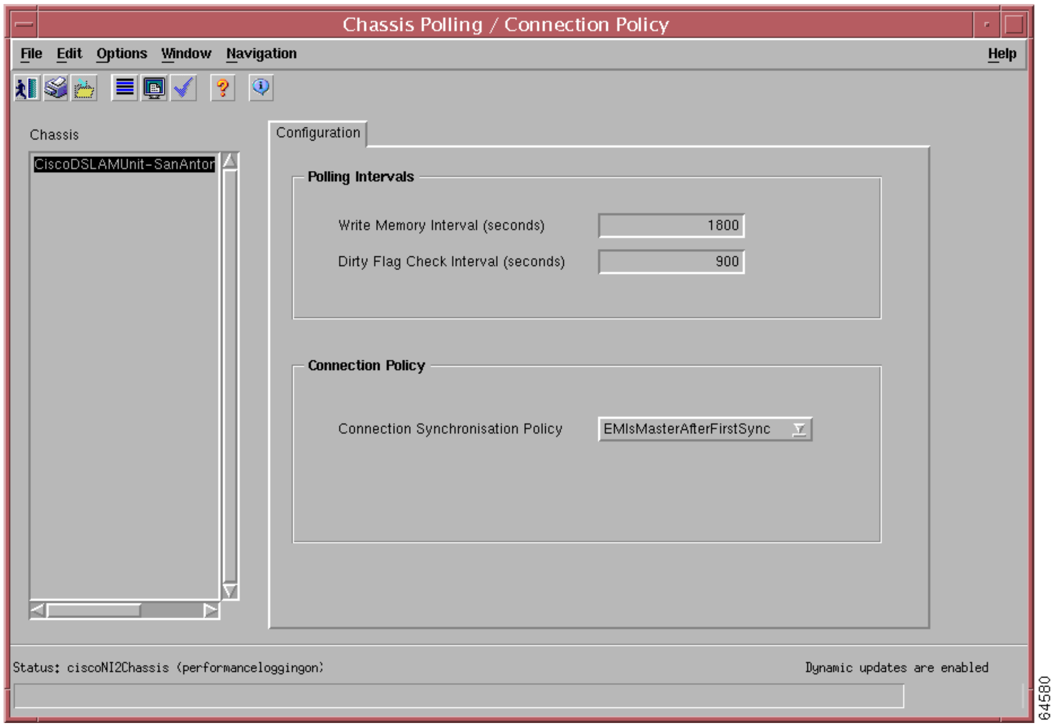
Complete the following steps to set the connection synchronization policy:

Step 1 On the Map Viewer window, within the Physical view, click the chassis object whose connection policy you want to set to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > Chassis Polling/Connection Policy**.

The Chassis Polling/Connection Policy window opens. (See Figure 4-5.)

Figure 4-5 Chassis Polling/Connection Policy Window



Step 3 In the Connection Policy area, use the down arrow in the Connection Synchronization Policy field to set the policy from one of the following choices:

- **Normal**—No action. The DSLAM is master, but do not add a connection to or delete a connection from CDM.
- **DeviceisMaster**—This setting specifies that the DSLAM (device) is the reference point for PVC creations and deletions. CDM will sync up to the device. If a connection is present on the DSLAM but not in CDM, CDM will create the connection. If a connection is absent on the DSLAM but present in CDM, CDM will delete the connection.
- **EMIsMasterAfterFirstSync**—The default. This setting specifies that the element manager, that is, CDM, is the reference point for PVC creations and deletions. The device syncs up to CDM for information about PVC settings. If the connection is present in CDM but not the DSLAM, CDM creates the connection in the DSLAM. If the connection is absent in CDM but present in the DSLAM, CDM deletes the connection from the DSLAM.

Step 4 Click the **Save** icon in the toolbar to save this setting.

Creating ATM QoS Profiles

This section includes the following topics:

- Opening the ATM QoS Profiles Configuration Window, page 4-8
- Creating an ATM QoS Profile, page 4-10
- Deleting an ATM QoS Profile, page 4-12

The Cisco DSLAM contains default ATM QoS profiles. ATM QoS profiles are also known as ATM traffic descriptors. You can create and save ATM QoS profiles in the QoS Profiles window. CDM stores ATM QoS profiles and creates the parameters on the device when CDM creates the PVC or SPVC.

Note After you create an ATM QoS profile, you can only edit that profile if it is not applied to a port. If a profile has been applied to a specific port, CDM prevents you from altering the profile. You can view the ports that are using a certain profile by running a Cisco EMF query against the profile name. (Refer to the *Cisco Element Management Framework User Guide* for details.)

Opening the ATM QoS Profiles Configuration Window

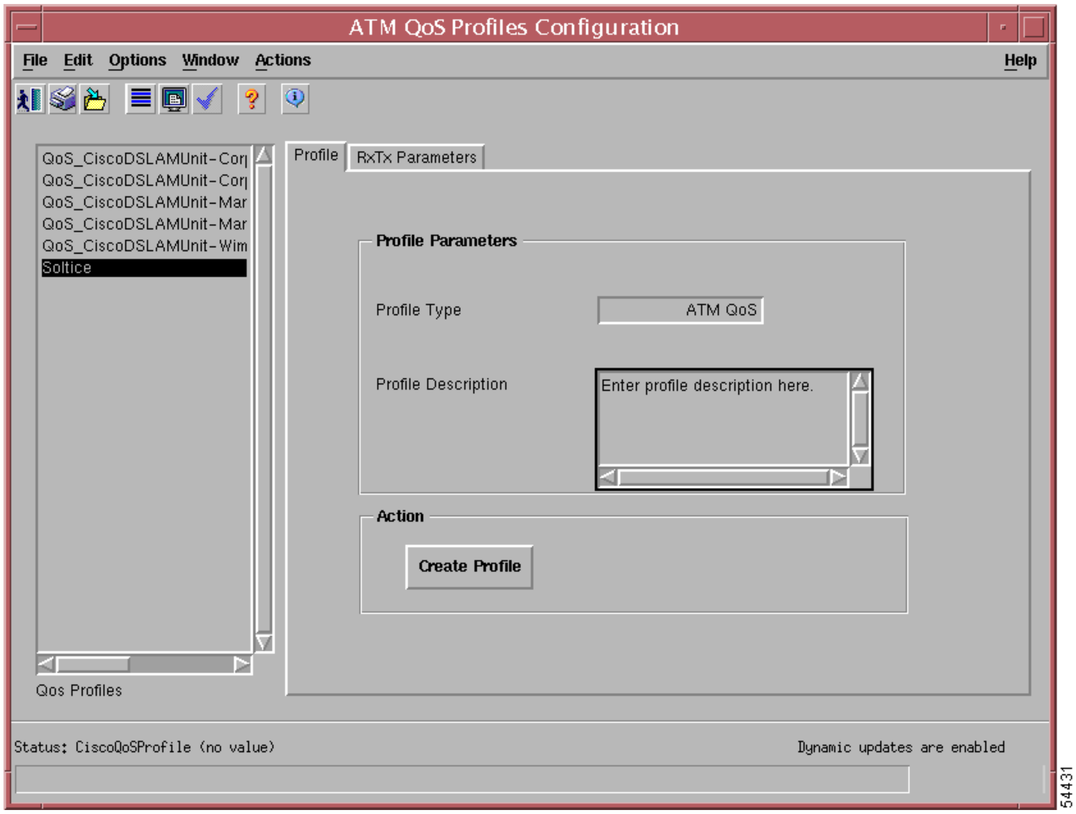
To create an ATM QoS profile, first open the ATM QoS Profiles Configuration window:

Step 1 From the left side of the Map Viewer window, within any view, right-click the chassis object for which you want to create an ATM QoS profile.

Step 2 Choose **Cisco DSL Manager > Chassis > Profile Management > ATM QoS Profiles** from the object menu.

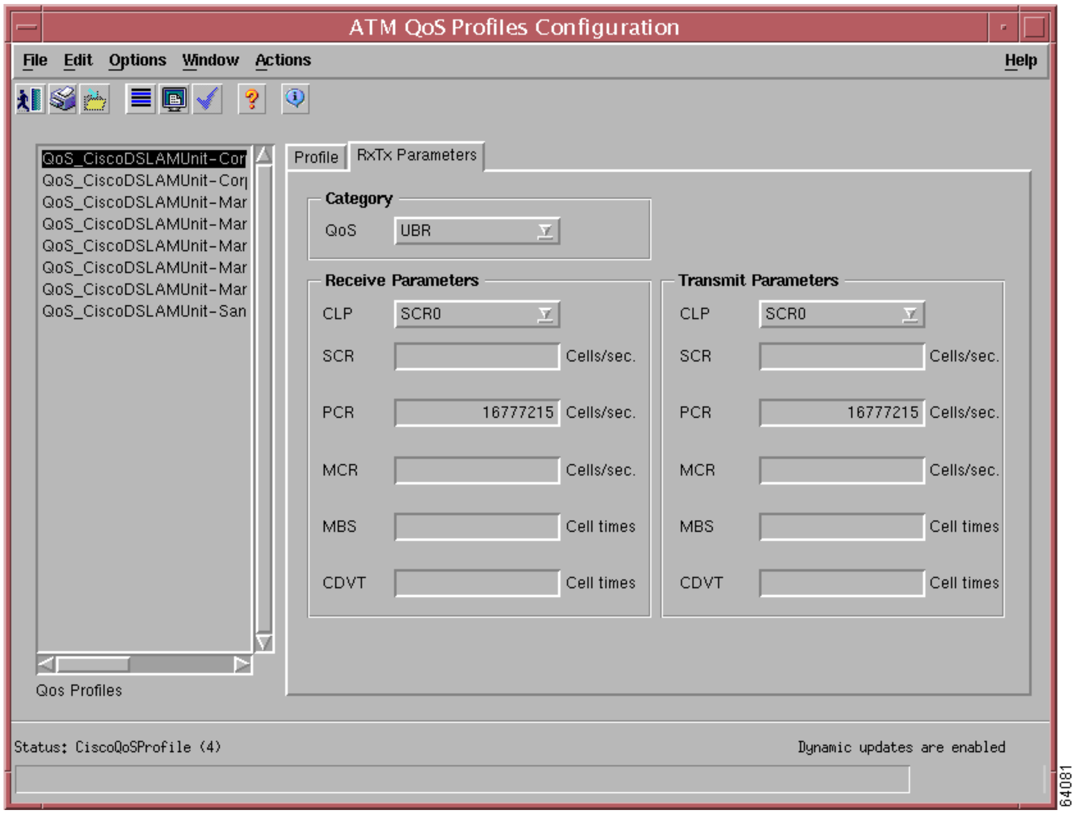
The ATM QoS Profiles Configuration window opens. (See Figure 4-6.)

Figure 4-6 ATM QoS Profiles Configuration Window—Profile Tab



The ATM QoS Profiles Configuration window contains two tabs—Profile and RxTx Parameters. The ATM QoS Profiles Configuration window opens to the Profile tab. The RxTx Parameters tab, which is shown in Figure 4-7, contains the receive and transmit parameters for the selected ATM QoS profile.

Figure 4-7 ATM QoS Profiles Configuration Window—RxTx Parameters Tab



Creating an ATM QoS Profile

Complete the following steps to create a new ATM QoS profile in the ATM QoS Profiles window:

Step 1 Select the profile that you want to use as a template from the list box in the left side of the window.

Step 2 Click **Create Profile**.

Step 3 Enter the new profile name in the Prompt dialog box, and then click **OK**.

Step 4 Enter the appropriate information in the required fields in the Profile tab as follows:

a. In the Profile Type field, enter the type of profile that you are creating, for example, ATM QoS profile.

b. In the Profile Descriptions field, enter a description for this profile.

Use the horizontal and vertical scroll bars to navigate.

Step 5 Click the **RxTx Parameters** tab, and enter the parameters that you want to set in this tab in either the Receive Parameters area or the Transmit Parameters area:

a. Use the down arrow to select from the choices in the QoS Category field, which indicates the current QoS category of the selected profile—either SCR0 or SCR10.

The type of CLP (cell loss priority) that you choose causes certain fields in the Receive Parameters and Transmit Parameters areas to become dimmed. Only those parameters that are valid for the type of CLP you choose are editable.

b. Enter a value in the CLP field, which indicates the value in the ATM cell header that determines the probability of the network dropping a cell if the network becomes congested.

Valid parameter choices include:

Parameter	Choices
ABR[1]	pcr[2], mcr[3], cdvt[4]
CBR[5]	pcr, cdvt
UBR[6]	pcr, mcr, cdvt
VBR-RT[7]	scr[8], pcr, mbs[9], cdvt
VBR-NRT[10]	scr, pcr, mbs, cdvt

1. ABR = available bit rate
2. PCR = peak cell rate
3. MCR = maximum cell rate
4. CDVT = cell delay variation tolerance
5. CBR = constant bit rate
6. UBR = unspecified bit rate
7. VBR-RT = variable bit rate real time
8. SCR = sustained cell rate
9. MBS = maximum burst size
10. VBR-NRT = variable bit rate not real time

Cells that have 0 (zero) in the CLP field have ensured priority and are unlikely to be dropped. Cells with 1 in the CLP field have best-effort priority and might be dropped during periods of congestion so that resources are free to handle ensured traffic.

c. Enter a value in the SCR field to specify the maximum sustained-cell-rate (scr) traffic parameter in cells per second that is allowed for connections.

d. Enter a value in the PCR field to specify the maximum transmission rate of cells in cells per second.

e. Enter a value in the MCR field to specify the lowest acceptable transmission rate for connections in cells per second.

f. Enter a value in the MBCS field to specify the maximum burst cell size permitted for cells received for connections on this interface in cell times.

g. Enter a value in the CDVT field to specify the estimated cell delay variation experienced by cells for connections received on this interface in cell times.

Step 6 Click **Save** to save your changes.

Deleting an ATM QoS Profile

To delete an existing ATM QoS profile, complete the following steps in the ATM QoS Profiles Configuration window:

Step 1 Right-click the profile name you want to delete in the list box.

Step 2 Choose **Deployment > Delete Objects**.

The Deployment Wizard Summary window opens.

Step 3 Click **Finish** to delete the selected object.

A message displays to confirm successful deletion.

Note You cannot delete a profile that is currently in use. To view the ports that use a specific profile, you can run a Cisco EMF query against the profile name (refer to the *Cisco Element Management Framework User Guide* for details.)

Creating PVCs and SPVCs

This section includes the following topics:

- Guidelines for Configuring ATM Virtual Channels, page 4-12
- Creating PVCs and SPVCs Overview, page 4-13
- Creating ATM PVCs, page 4-13
- Deploying ATM SPVCs with a Cisco EMF Endpoint, page 4-21
- Deploying an ATM SPVC with a non-Cisco EMF Endpoint, page 4-27
- Activating the PVC or SPVC Connection, page 4-37

A PVC is a permanent virtual connection that must be configured from source to destination. PVCs save bandwidth that is associated with establishing a channel when a virtual channel must exist all the time. You can deploy a PVC or SPVC (which creates the PVC/SPVC within Cisco EMF), apply a QoS profile (ATM traffic descriptor) to the PVC or SPVC, and then create the connection on the device. Deploying and creating a PVC creates a cross connection within one device; deploying and creating an SPVC creates a connection between the incoming port on one device and the outgoing port on another device.

Note After you create a PVC or an SPVC, you can only view the channel within the Component Managed view. The channel does not appear in the other Map Viewer Element Manager views.

Guidelines for Configuring ATM Virtual Channels

Service provisioning for ATM must adhere to a variety of configuration standards, which prevent errors when establishing ATM connections. CDM includes service provisioning logic to ensure valid combinations of configuration data.

Consider the following guidelines before you configure ATM virtual channels:

- You can provision more than one permanent virtual connection (PVC) for each subscriber.
- Each PVC contains both a network-side and a subscriber-side virtual channel link (VCL).
- Each VCC has both a VPI and a VCI.
- VPC switching is not supported in this release.
- If you enter VCI numbers, you must also enter VPI numbers.

Creating PVCs and SPVCs Overview

You can create PVCs or SPVCs to specify an ATM connection. You can choose from the following types of ATM connections in the Deployment Wizard—Templates window:

- PVC and virtual channel link (VCL) under ATM switch
- PVC and VCL under ATM switch using trunk port
- SPVC with Cisco EMF endpoint
- SPVC with non-Cisco EMF endpoint

Creating ATM PVCs

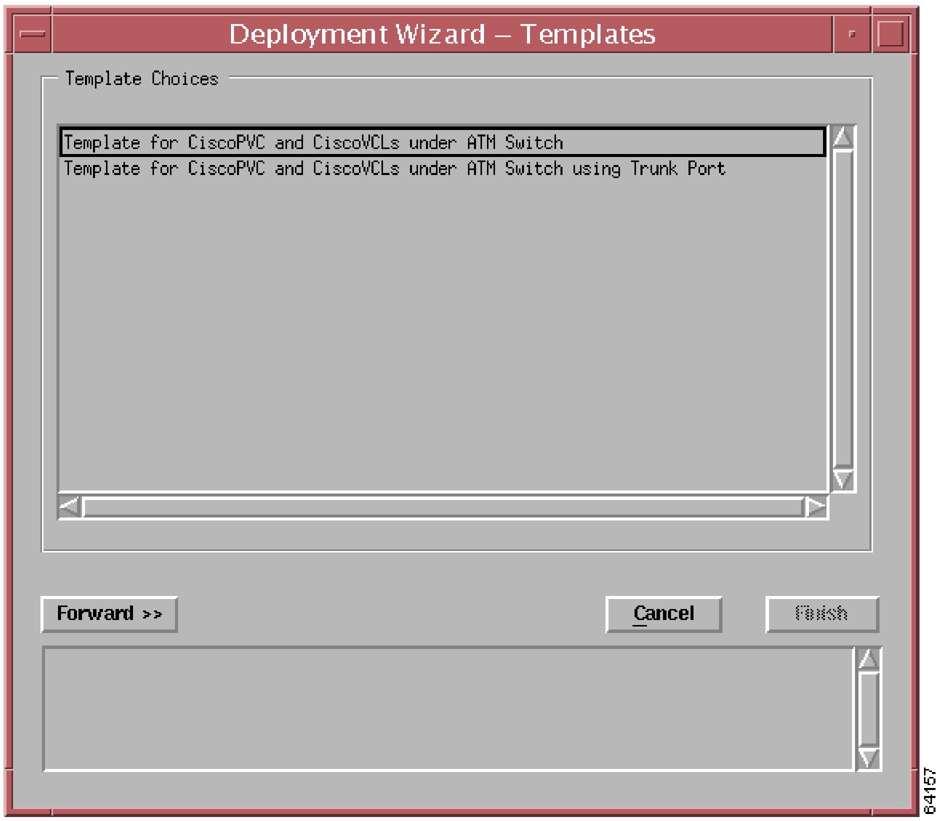
Complete the following steps to deploy an ATM PVC and VCL under an ATM switch or under an ATM switch using a trunk port:

Step 1 From the Component Managed view, right-click over the interface for which you want to deploy an ATM PVC and VCL connection to access the object menu.

Step 2 Choose **Deployment > Deploy ATM Connection > PVC**.

The Deployment Wizard—Templates window opens. (See Figure 4-8.)

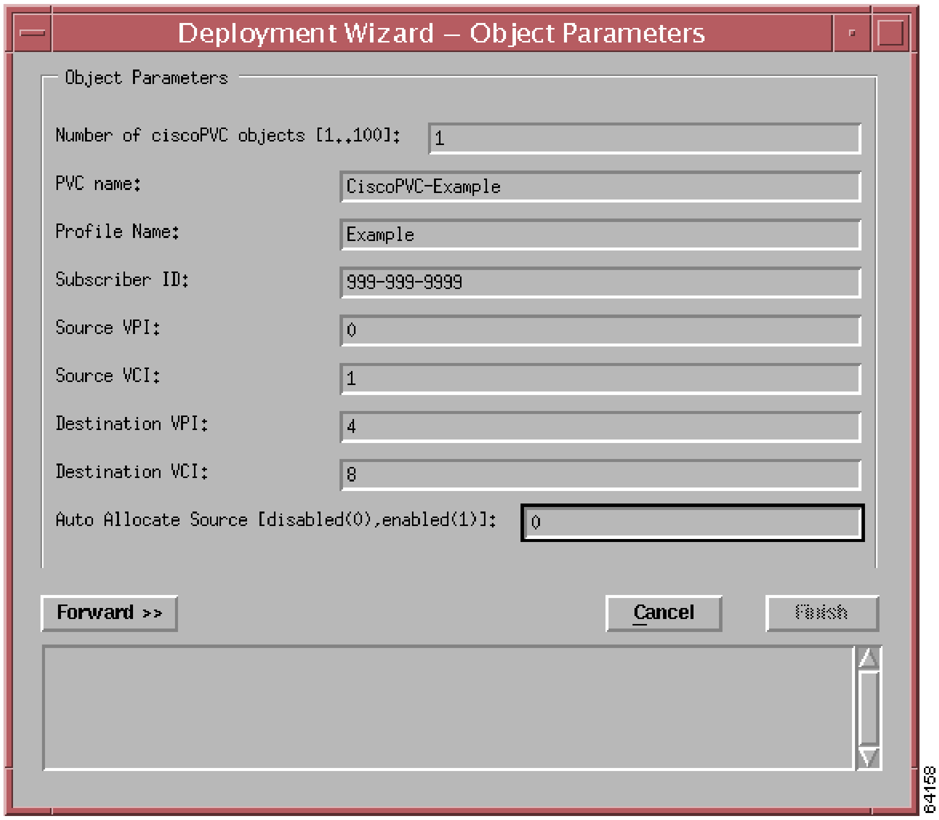
Figure 4-8   Deployment Wizard—Templates Window



Step 3 Click either **Template for CiscoPVC and CiscoVCLs under ATM Switch** or **Template for CiscoPVC and CiscoVCLs under ATM Switch using Trunk Port** to highlight your choice, and then click **Forward**.

The Deployment Wizard—Object Parameters window opens. (See Figure 4-9.)

Figure 4-9 Deployment Wizard—Object Parameters Window



Tip You can use the Tab key to move from one field to the next.

Step 4 Enter the appropriate information in the Object Parameters fields as follows:

a. Enter the number of SPVC objects that you want to deploy from 1 to 100 in the Number of ciscoSPVC objects field.

The number that you enter into this field deploys that number of PVCs on the designated interface.

b. Enter the name you want to give the PVC in the PVC name field; make sure this name in unique.

c. Enter the QoS profile name for the PVC you are deploying in the Profile Name field.

To view a list of the ATM QoS profiles, open the ATM QoS Profiles Configuration window by choosing **Cisco DSL Manager > Chassis > Profile Management > ATM QoS Profiles** from the object menu.

d. Enter the subscriber ID in the Subscriber ID field, or you can leave this value undefined.

e. Enter the number of the subscriber-side VPI in the Source VPI field.

f. Enter the number of the subscriber-side VCI in the Source VCI field.

g. Enter the number of the network-side VPI in the Destination VPI field.

h. Enter the number of the network-side VCI in the Destination VCI field.

If you set the values in the VPI and VCI fields, you must disable auto allocation. If you want to enable auto allocation, leave the VPI and VCI fields blank.

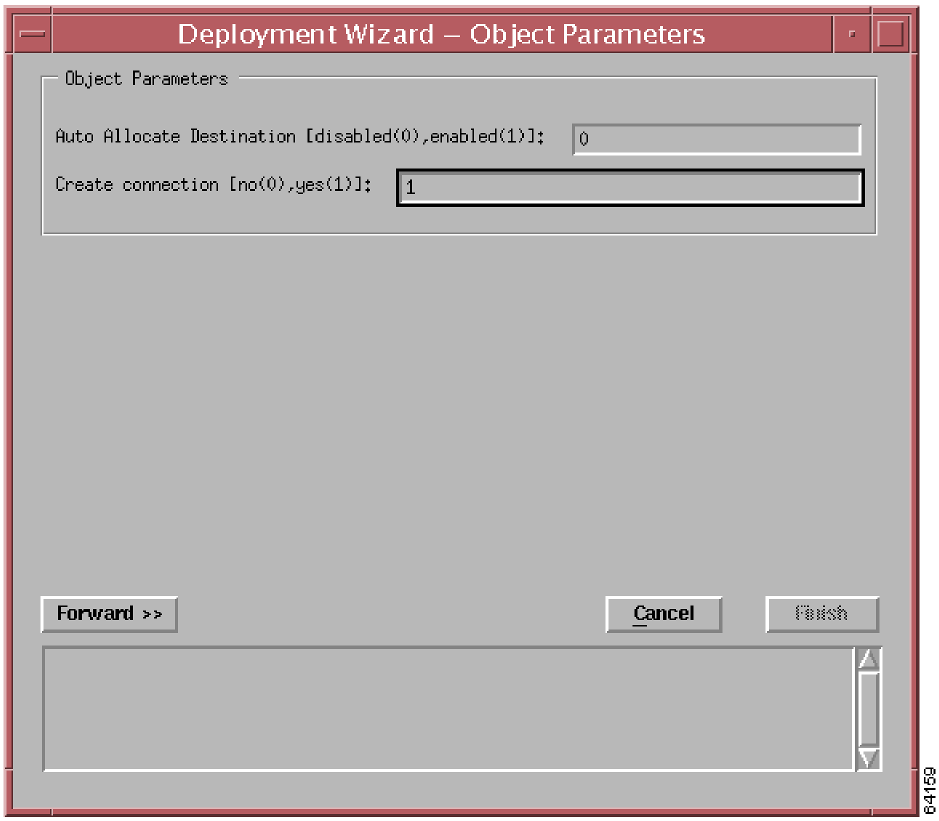
i. Leave the default, **0,** to disable auto allocation or enter **1** to enable autoallocation in the Auto Allocate Source field.

   Your choice depends on whether you want CDM to automatically allocate the VPIs and VCIs.

j. Click **Forward** to continue.

The next Deployment Wizard—Object Parameters window opens. (See Figure 4-10).

Figure 4-10 Deployment Wizard—Object Parameters Window



Step 5 Enter **0** for disable or **1** for enable in the Auto Allocate Destination field to specify whether you want CDM to autoallocate the destination address.

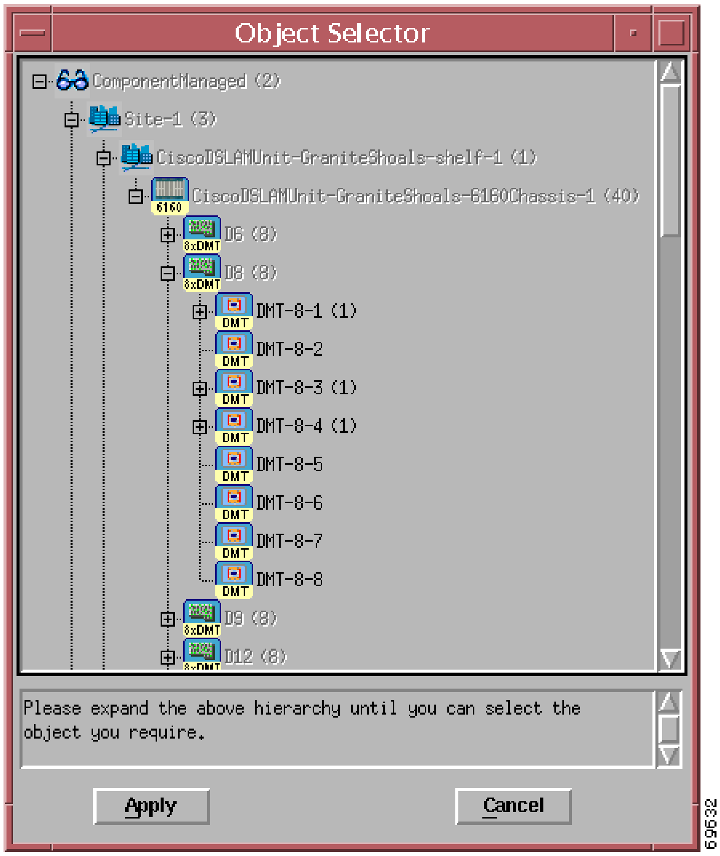
Step 6 Enter **1** for yes in the Create connection field to specify that you want CDM to create the connection.

Step 7 Click **Forward** to continue.

The Deployment Wizard—Views window opens. If you are deploying an ATM Connection PVC under ATM Switch, this window has two Component Managed fields. Each has a Select button next to it. If you are deploying an ATM Connection PVC under ATM switch using Trunk Port, this window has one Component Managed field with a Select button next to it.

Step 8 Click **Select** to open the Object Selector window opens. (See Figure 4-11.)

Figure 4-11 Object Selector Window



Step 9 Click **+** next to the objects that are listed to drill down to the source interface that you want to select for this PVC, then click **Apply**.

The Deployment Wizard—Views window opens again and displays the interface that you selected from the Object Selector window. You selection populates both fields.

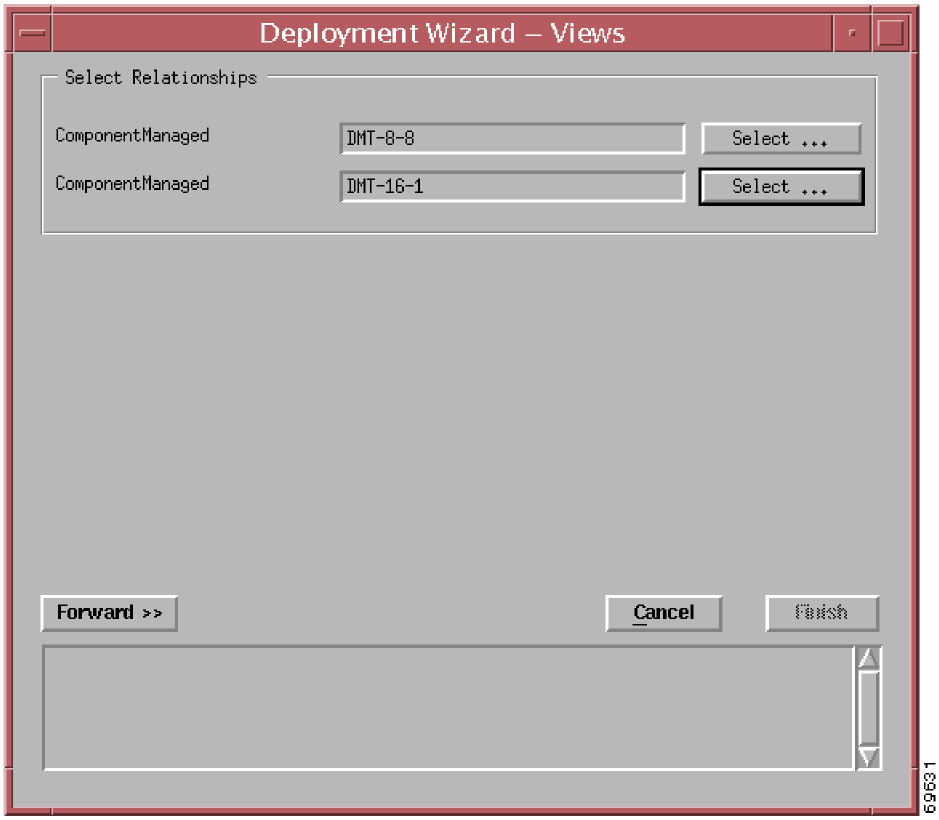
Note If you are deploying PVCs and VCLs under ATM and *not* using a trunk port, you must use a different selection for your outgoing port.

Step 10 Repeat Step 8 and Step 9 if the window displays a second Component Managed field to specify an outgoing port.

Note Skip Step 10 if you select the Template for Cisco PVC and Cisco VCLS under ATM Switch using Trunk Port. If you use this template, CDM automatically selects the trunk port for the network end of the PVC.

The Deployment Wizard—Views window displays the interfaces that you have selected. An example is shown in Figure 4-12.

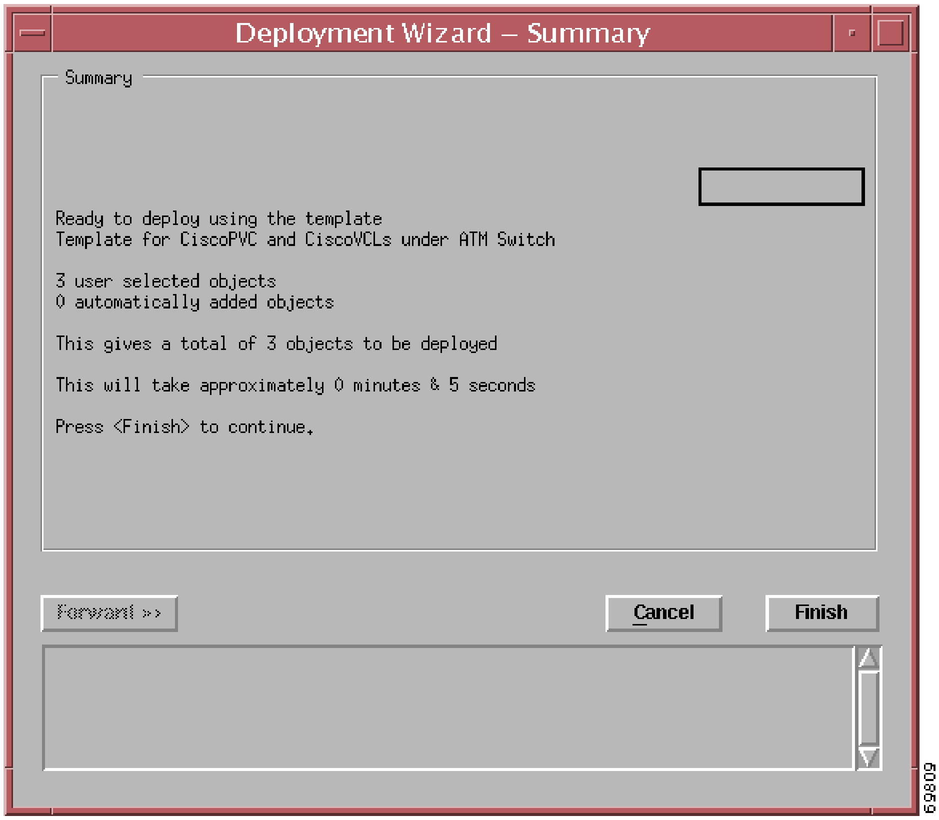
Figure 4-12 Example Deployment Wizard—Views Window



Step 11 Click **Forward** to continue.

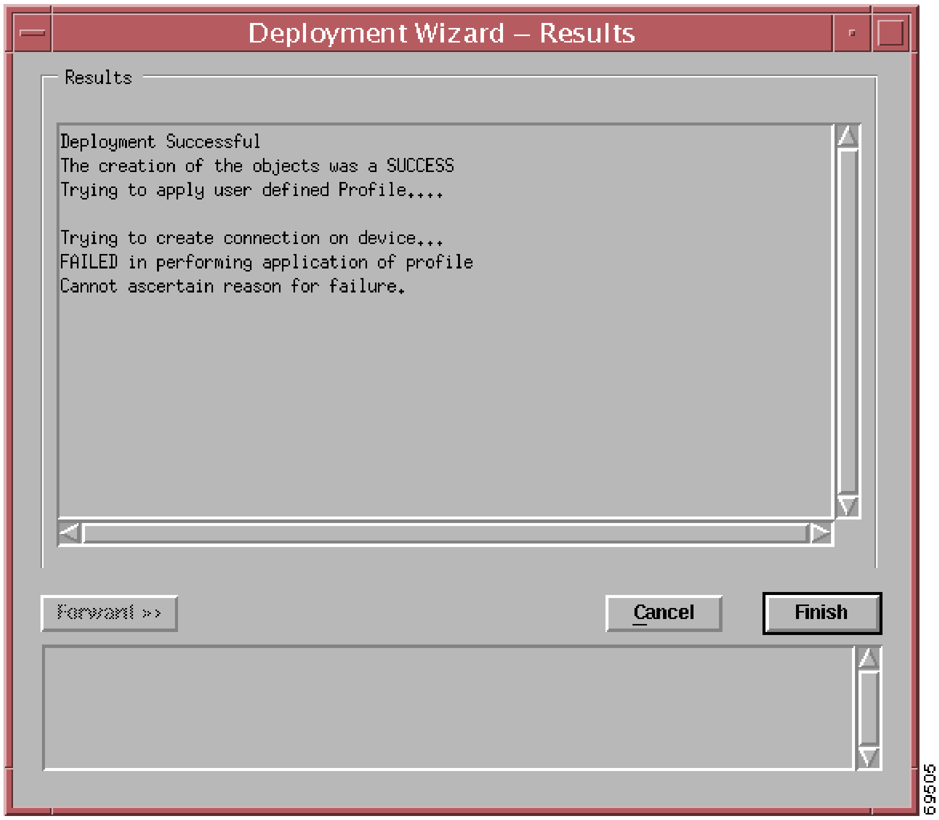
The Deployment Wizard—Summary window, which is shown in Figure 4-14, opens to inform you that the deployment process is ready and summarizes the deployment that you have selected.

Figure 4-13 Deployment Wizard—Summary Window



The Deployment Wizard—Results window, which is shown in Figure 4-14, opens and displays the results of the deployment.

Figure 4-14 Deployment Wizard—Results Window



Step 12 Click **Finish** to complete the deployment.

The Deployment Wizard—Summary window, which is shown in Figure 4-14, summarizes your deployment. In this example, the software failed to apply the profile. When you create a PVC or SPVC, the software creates two virtual channel links (VCLs) that represent the two incoming and outgoing endpoints.

You need to verify that CDM completed the following three tasks:

- Created the PVC
- Applied to the ATM QoS profile
- Completed the connection

If CDM failed to complete any of these tasks, you must manually create the connection. See the "Creating PVCs and SPVCs" section on page 4-12, "Applying an ATM QoS Profile to a PVC or SPVC" section on page 4-36, and the "Manually Uploading ATM QoS Profiles" section on page 4-49 for the related instructions.

Deploying ATM SPVCs with a Cisco EMF Endpoint

To deploy SPVCs with a Cisco EMF endpoint, complete the steps that follow. When you deploy an SPVC for which the endpoint is a network service that is not under the management of Cisco EMF (non-CEMF endpoint), you deploy the SPVC in a different way.

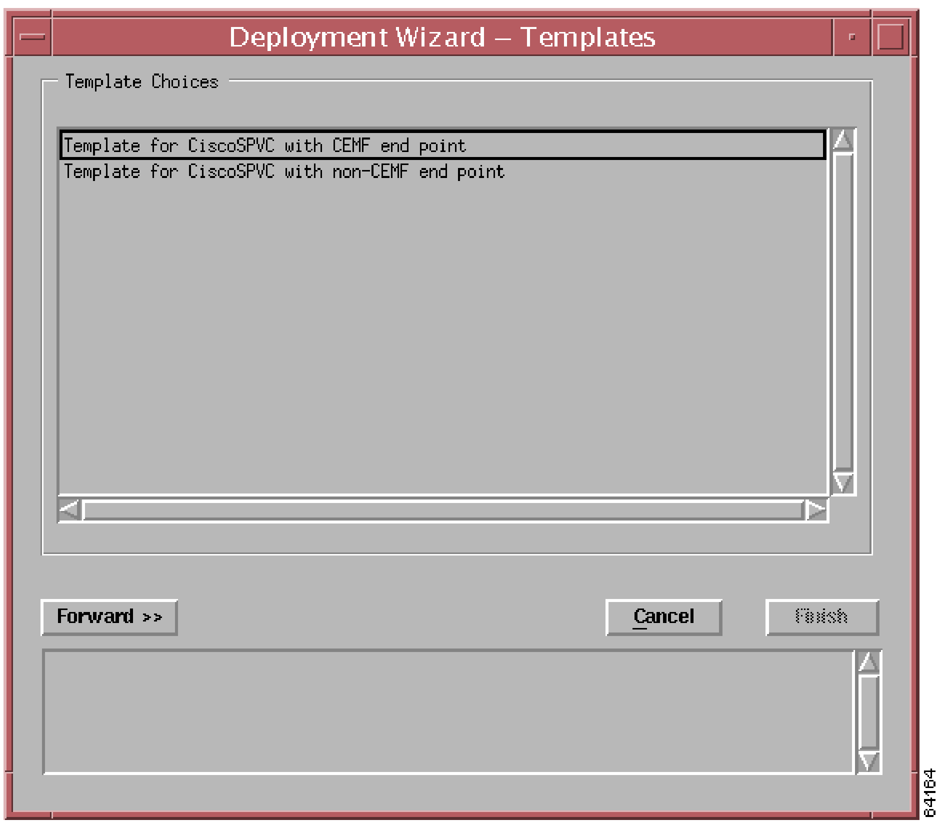
Note To create an SPVC that has a non-Cisco EMF endpoint, see the "Deploying an ATM SPVC with a non-Cisco EMF Endpoint" section on page 4-27.

Step 1 From the left side of the Map Viewer window, right-click the chassis object for which you want to create a PVC or SPVC.

Step 2 Choose **Deployment > Deploy ATM Connection > SPVC** from the object menu.

The Deployment Wizard—Templates window opens. An example of this window is shown in Figure 4-15.

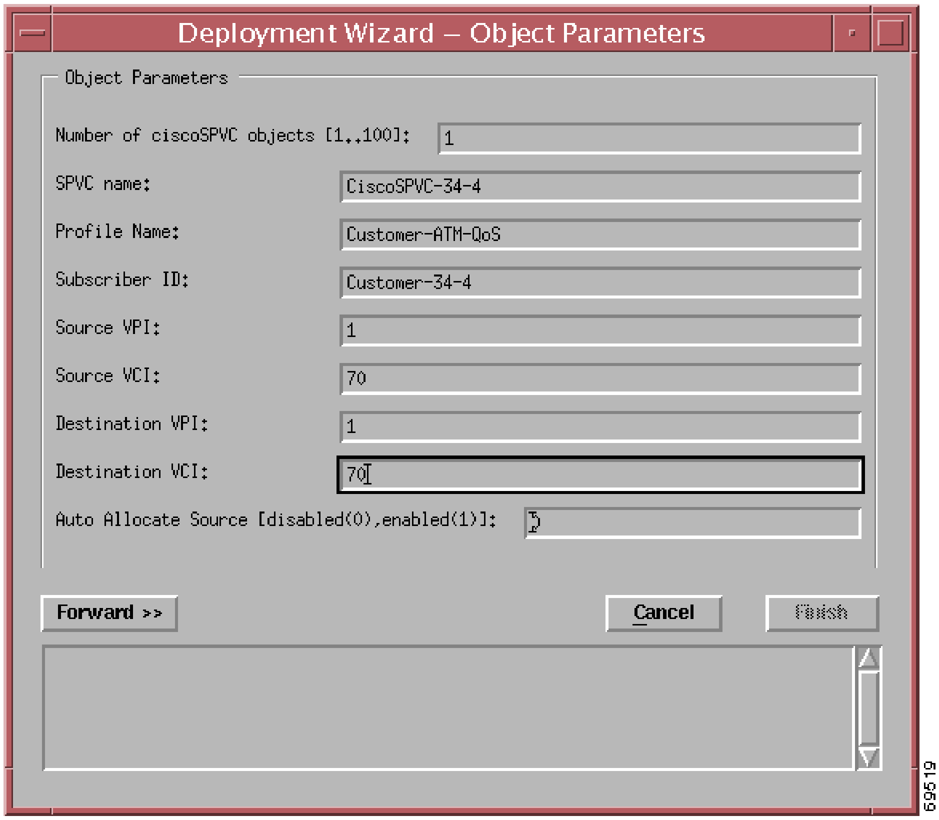
Figure 4-15 Deployment Wizard—Templates Window for Deploying an ATM SPVC



Step 3 Click **Template for Cisco SPVC with CEMF end point**.

The Deployment Wizard—Object Parameters window opens. (See Figure 4-16.)

Figure 4-16 Deployment Wizard—Object Parameters Window ATM SPVC with a CEMF Endpoint



Tip You can use the Tab key to move from one field to the next.

Step 4 Enter the appropriate choices as follows:

- **a.** Enter **1** in the number of SPVC objects that you want to deploy in the Number of ciscoSPVC objects field.
- **b.** Enter the SPVC name in the SPVC name field; make sure that the name you choose is unique.
- **c.** Enter the name of the profile that you want to use in the Profile field, or use the default by leaving Default in this field.
- **d.** Enter the subscriber ID in the Subscriber ID field, or leave this value undefined.
- **e.** Enter the subscriber-side VPI in the Source VPI field.
- **f.** Enter the subscriber-side VC in the Source VCI field.
- **g.** Enter the network-side VPI in the Destination VPI field.
- **h.** Enter the network-side VCI in the Destination VCI field.

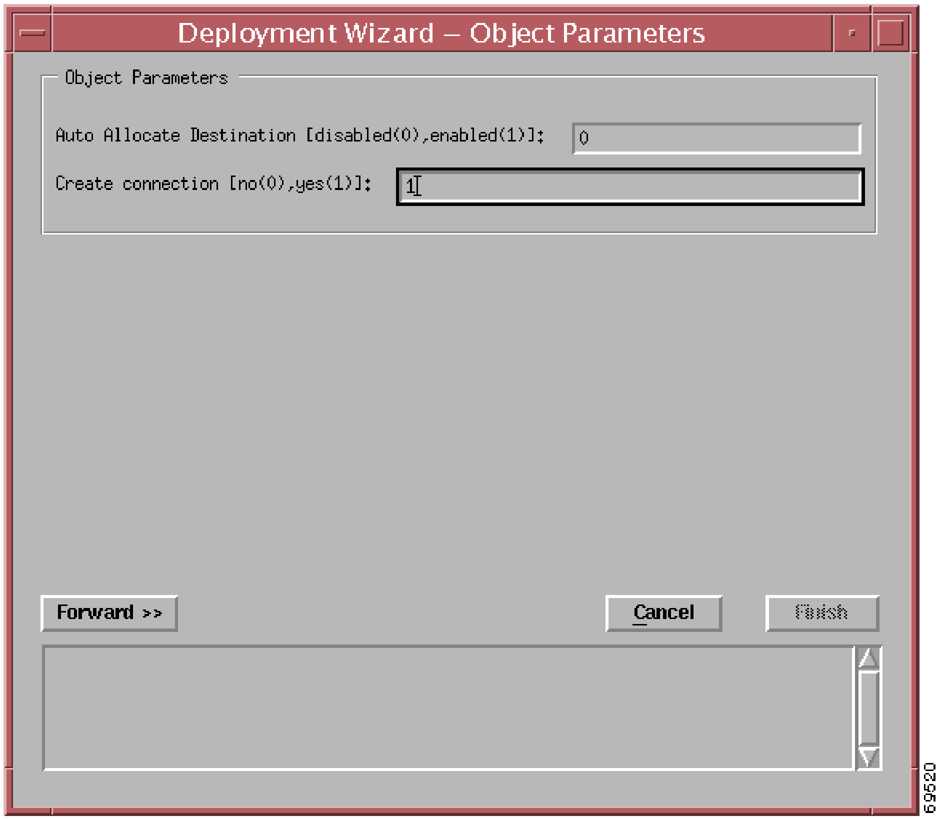
  If you set the values in the VPI and VCI fields, you must disable auto allocation. If you want to enable auto allocation, leave the VPI and VCI fields blank.

i. Enter a **0** to disable autoallocation or **1** to enable autoallocation in the Auto Allocate Source field depending on whether you want CDM to automatically allocate the VPIs and VCIs.

j. Click **Forward** to continue.

The next Deployment Wizard—Object Parameters window opens. (See Figure 4-17.)

Figure 4-17 Deployment Wizard—Object Parameters Window



Step 5 Enter **0** for disable or **1** for enable in the Auto Allocate Destination field to specify whether you want CDM to autoallocate the destination address.

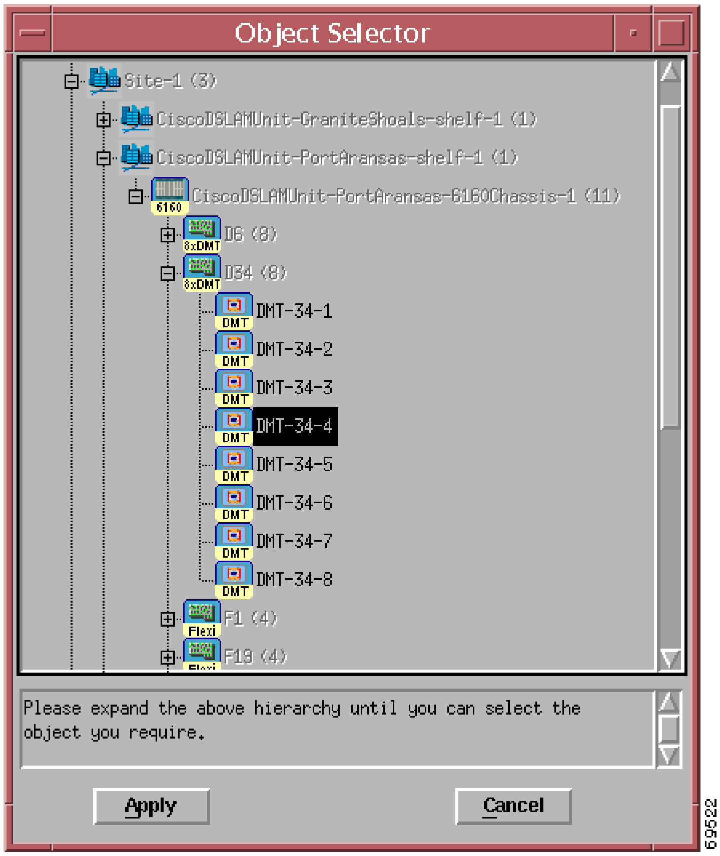
Step 6 Enter **1** for yes in the Create connection field to specify that you want CDM to create the connection.

Step 7 Click **Forward** to continue.

The Deployment Wizard—Views window opens. This window has two Component Managed fields. Each has a Select button next to it.

Step 8 Click **Select** to open the Object Selector window opens. (See Figure 4-18.)

Figure 4-18 Object Selector Window



Step 9 Click **+** next to the objects that are listed to drill down to the interface that you want to select for this PVC, then click **Apply**.

The Deployment Wizard—Views window opens again and displays the interface that you selected from the Object Selector window.

Step 10 Repeat Step 8 and Step 9 if the window displays a second Component Managed field and consider the following guidelines:

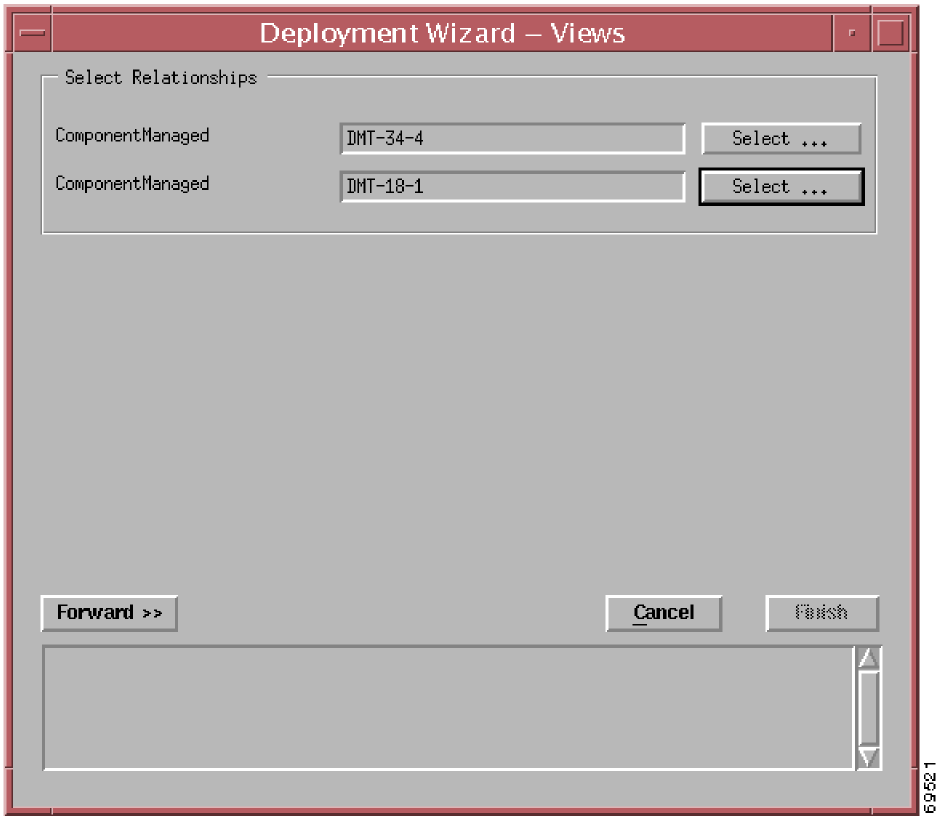
a. If the port is a CEMF endpoint, you must select an NI-2 port from another DSLAM.

b. If the port is a non-CEMF endpoint, you must select another network address.

Note If you do not select the correct ports in the Object Selector window, your SPVC deployment fails.

The Deployment Wizard—Views window displays the interfaces that you have selected. An example of this window is shown in Figure 4-19.

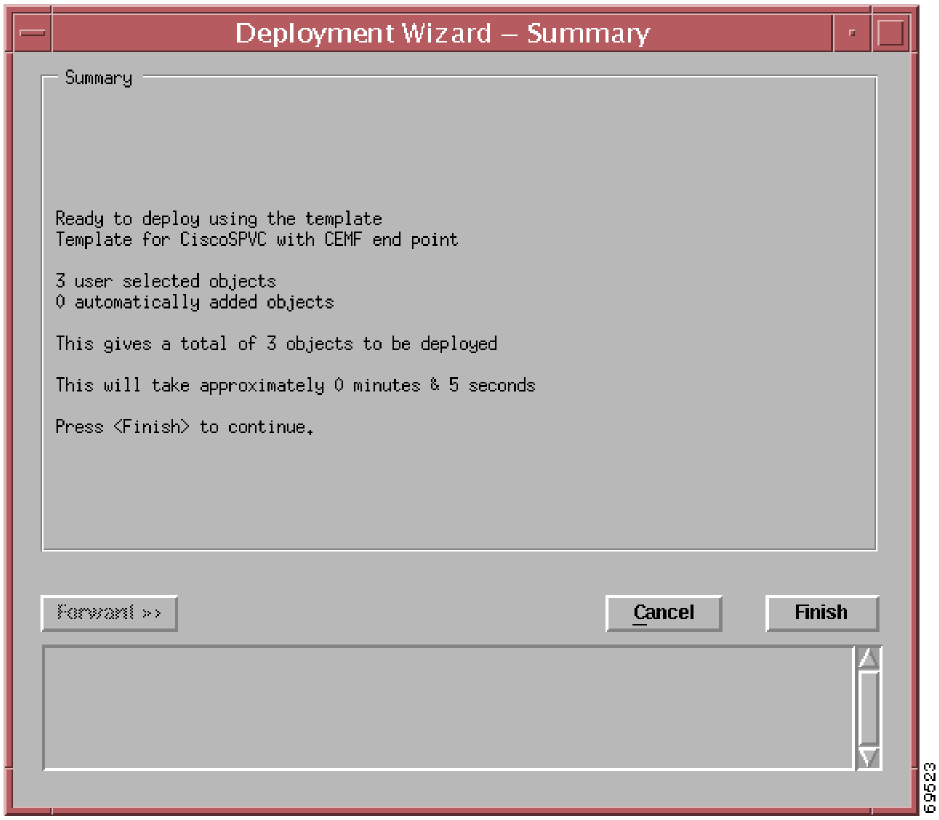
Figure 4-19 Example of a Deployment Wizard—Views Window



Step 11 Click **Forward** to continue.

The Deployment Wizard—Summary window, which is shown in Figure 4-20, opens and displays the deployment action that is to take place.

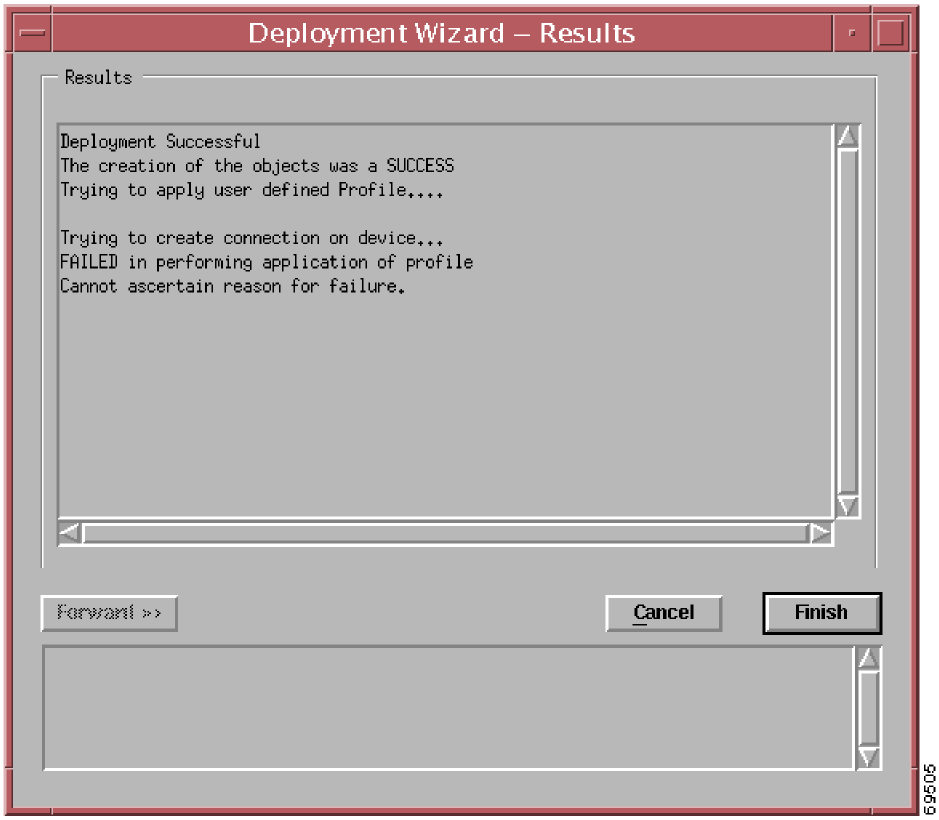
Figure 4-20 Deployment Wizard—Summary Window



Step 12 Click **Finish** to complete the deployment.

The Deployment Wizard—Results window opens. (See Figure 4-21.)

Figure 4-21 Deployment Wizard—Results Window



The Deployment Wizard—Summary window, which is shown in Figure 4-20, summarizes your deployment. In this example, the software failed to apply the profile. When you create a PVC or SPVC, the software also creates two virtual channel links (VCLs) that represent the two incoming and outgoing endpoints.

You can configure and view status and performance for these VCLs. The procedure for doing this is described in the "Managing VCLs" section on page 4-39.

Deploying an ATM SPVC with a non-Cisco EMF Endpoint

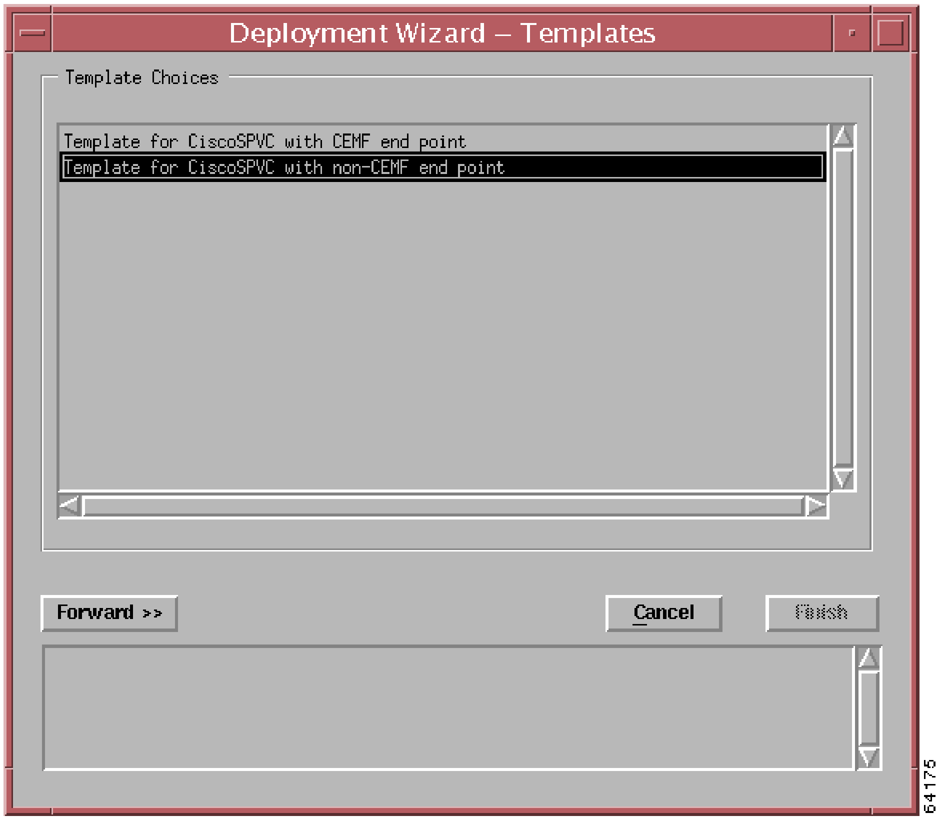
To deploy an SPVC for which the endpoint is a network service that is not under the management of Cisco EMF, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Component Managed view, right-click the chassis object for which you want to create a non-CEMF SPVC.

Step 2 Choose **Deployment > Deploy ATM Connection > SPVC** from the object menu.

The Deployment Wizard—Templates window opens. (See Figure 4-22.)

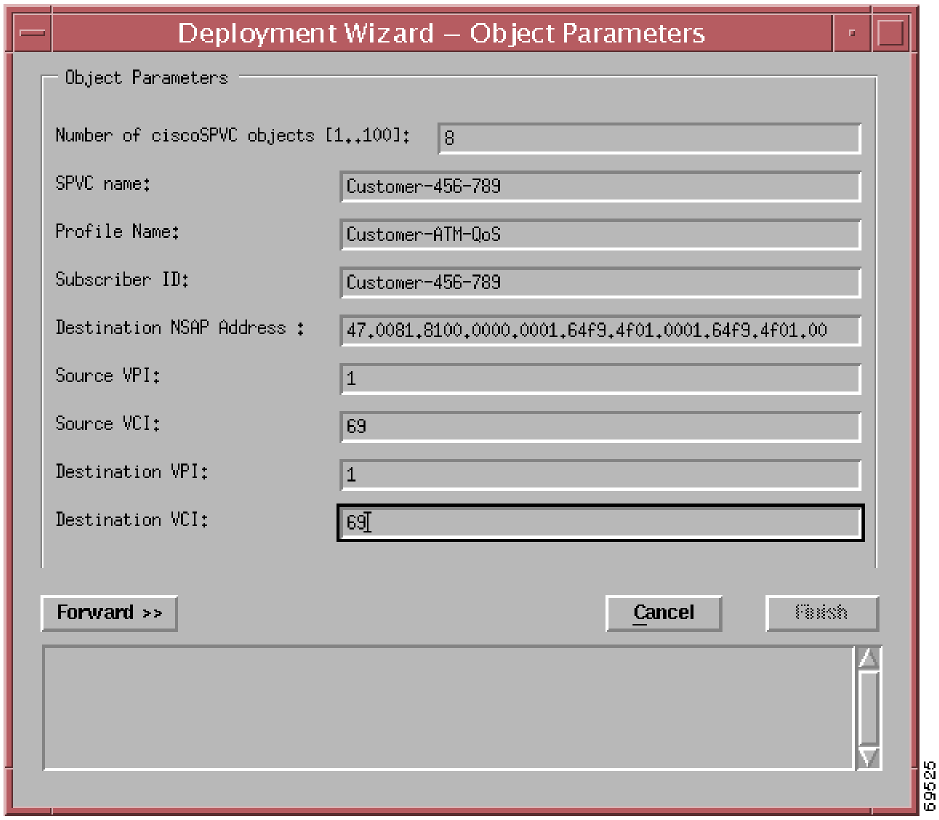
Figure 4-22 Deployment Wizard—Templates Window for Deploying an ATM SPVC



Step 3 Click **Template for Cisco SPVC with nonCEMF end point**.

The Deployment Wizard—Object Parameters window opens. (See Figure 4-23.)

Figure 4-23 Deployment Wizard—Object Parameters Window ATM SPVC with non-CEMF Endpoint



Tip You can use the Tab key to move from one field to the next.

Step 4 Enter the appropriate choices:

a. Enter the number of SPVC objects that you want to deploy from 1 to 100 in the Number of ciscoSPVC objects field.

If you enter 8, for example, in the Number of ciscoSPVC objects field, CDM deploys 8 SPVCs on that interface.

b. Enter the SPVC name in the SPVC name field; make sure that the name you choose is unique (not used by another SPVC).

c. Enter the subscriber ID in the Subscriber ID field or leave this value undefined.

d. Enter the destination network service access point (NSAP) address in the Destination NSAP address field.

If the non-CEMF endpoint runs Cisco IOS, you can obtain the destination NSAP address by using the **show atm address** command. This command displays a list of all of the ATM interfaces on a chassis and their NSAP addresses. Select the NSAP address from the network interface that you want to specify. For example, ATM 0/2.

e. Enter the name of the profile that you want to use in the Profile field, or use the default by leaving Default in this field.

f. Enter the subscriber-side VPI in the Source VPI field.

g. Enter the subscriber-side VC in the Source VCI field.

h. Enter the network-side VPI in the Destination VPI field.

i. Enter the network-side VCI in the Destination VCI field.

If you set the values in the VPI and VCI fields, you must disable auto allocation. If you want to enable auto allocation, leave the VPI and VCI fields blank.

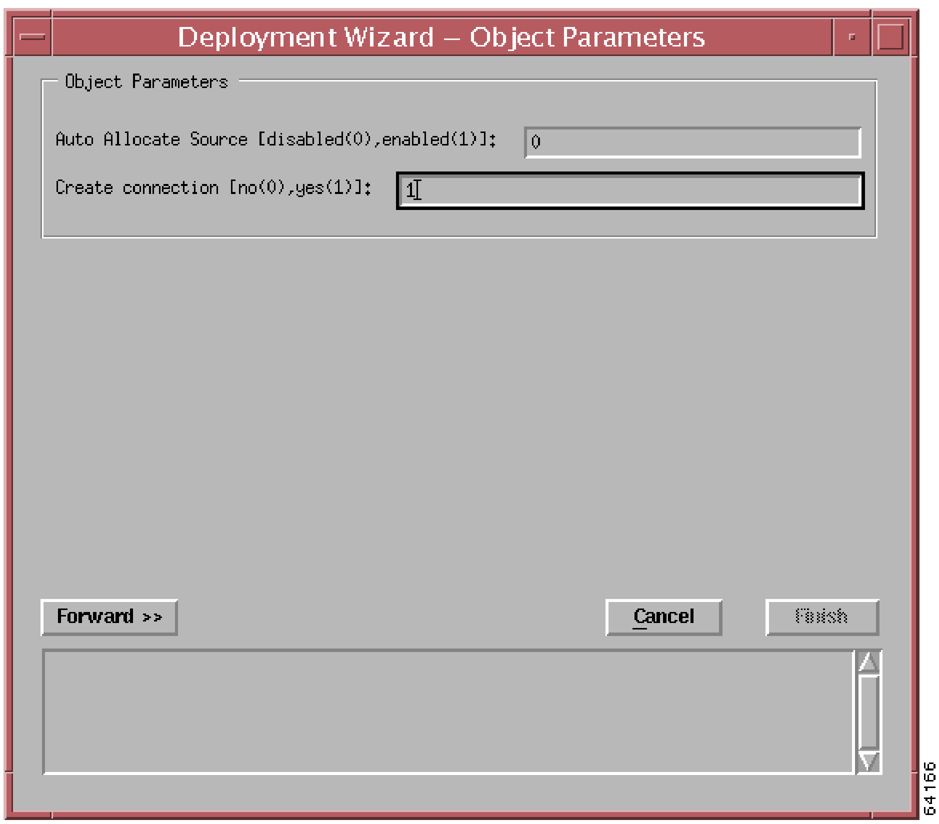
j. Enter a **0** to disable autoallocation or **1** to enable autoallocation in the Auto Allocate Source field depending on whether you want CDM to automatically allocate the VPIs and VCIs.

k. Enter **1** for yes in the Create connection field to specify that you want CDM to create the connection.

l. Click **Forward** to continue.

The next Deployment Wizard—Object Parameters window opens. (See Figure 4-24.)

Figure 4-24 Deployment Wizard—Object Parameters Window



Step 5 Leave the setting as **0** for disable in the Auto Allocate Destination field.

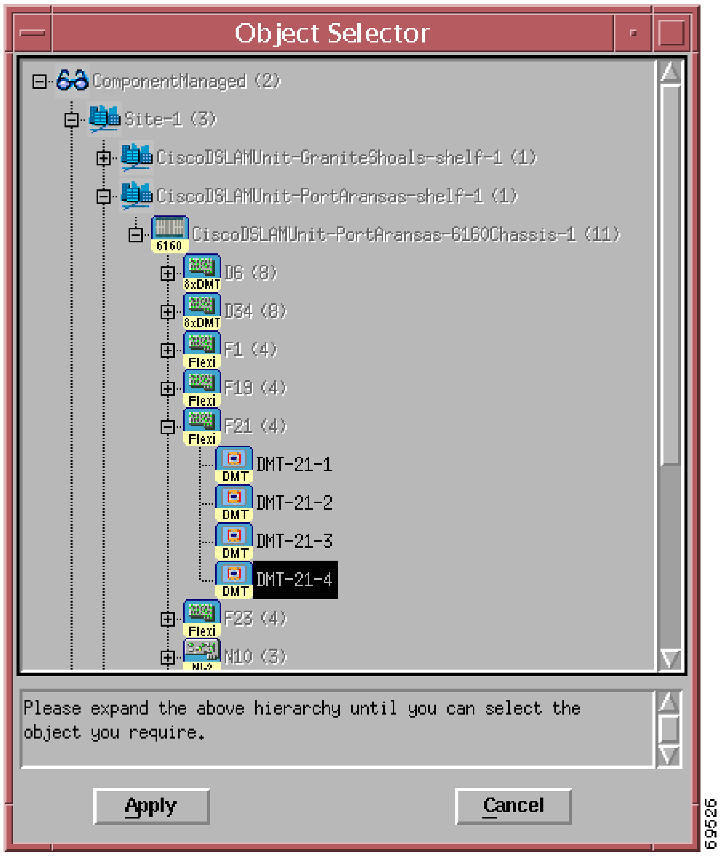
Step 6 Enter **1** for yes in the Create connection field to specify that you want CDM to create the connection.

Step 7 Click **Forward** to continue.

The Deployment Wizard—Views window opens. This window has two Component Managed fields. Each has a Select button next to it.

Step 8 Click **Select** to open the Object Selector window opens. (See Figure 4-25.)

Figure 4-25 Object Selector Window



Step 9 Click **+** next to the objects that are listed to drill down to the interface that you want to select for this PVC, then click **Apply**.

The Deployment Wizard—Views window opens again and displays the interface that you selected from the Object Selector window.

Step 10 Repeat Step 8 and Step 9 if the window displays a second Component Managed field and consider the following guidelines:

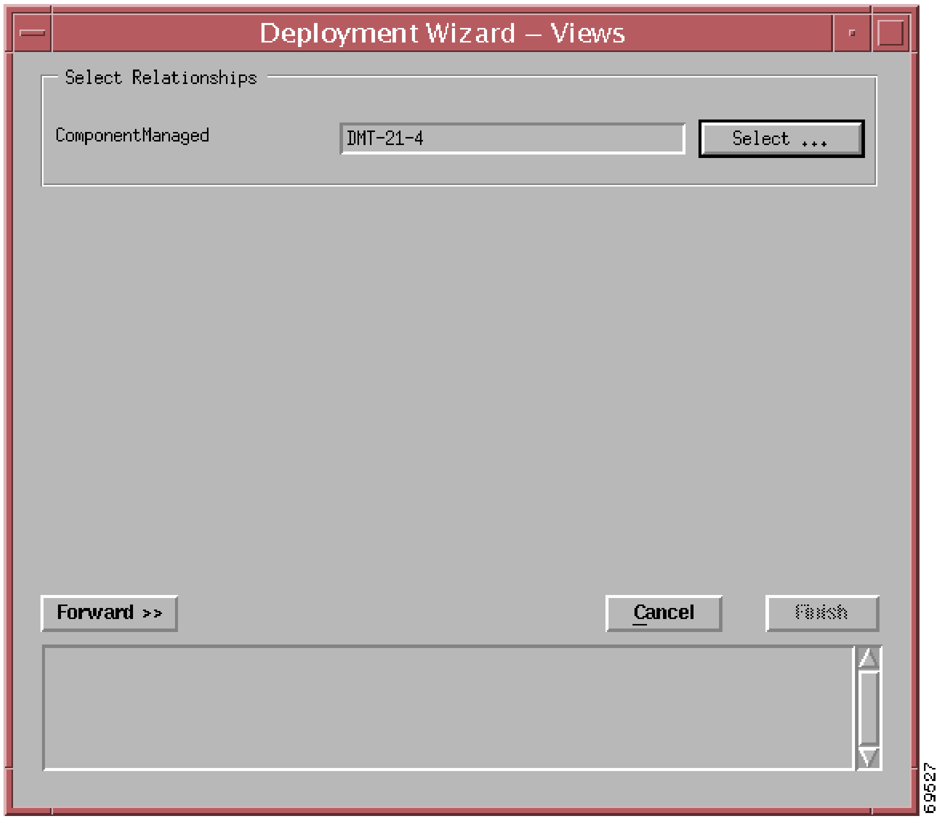
a. If the port is a CEMF endpoint, you must select an NI-2 port from another DSLAM.

b. If the port is a non-CEMF endpoint, you must select another network address.

Note If you do not select the correct ports in the Object Selector window, your SPVC deployment fails.

The Deployment Wizard—Views window displays the interfaces that you have selected. An example of this window is shown in Figure 4-26.

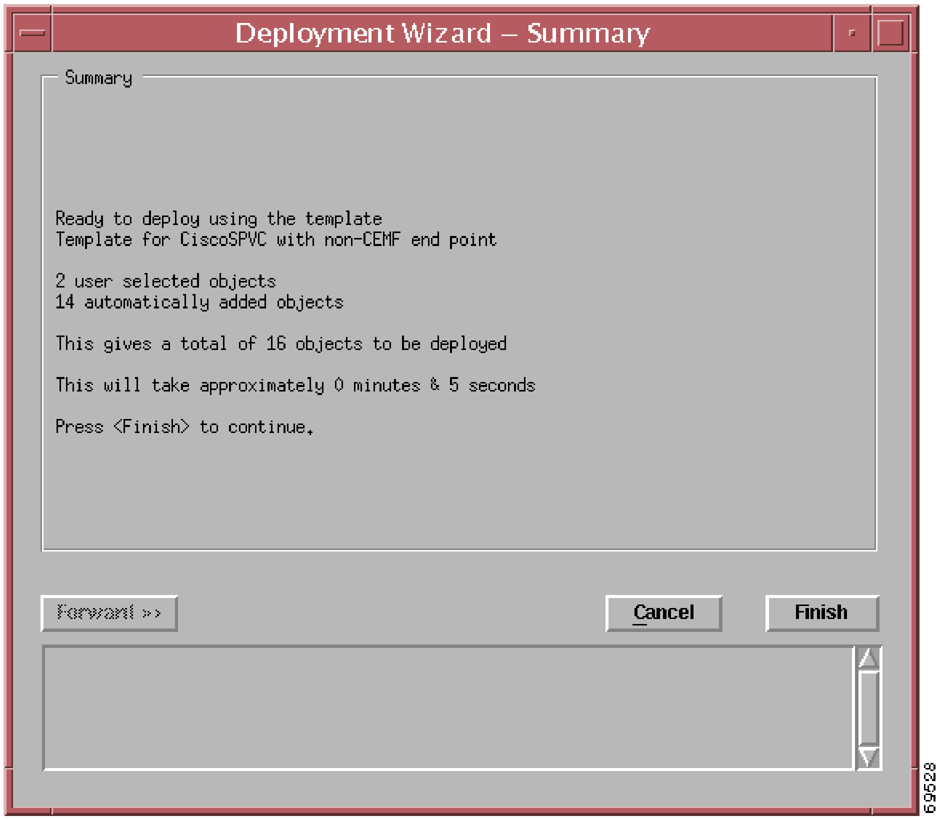
Figure 4-26 Example of the Deployment Wizard—Views Window



Step 11 Click **Forward** to continue.

The Deployment Wizard—Summary window opens and displays the deployment action that is to take place. (See Figure 4-20.)

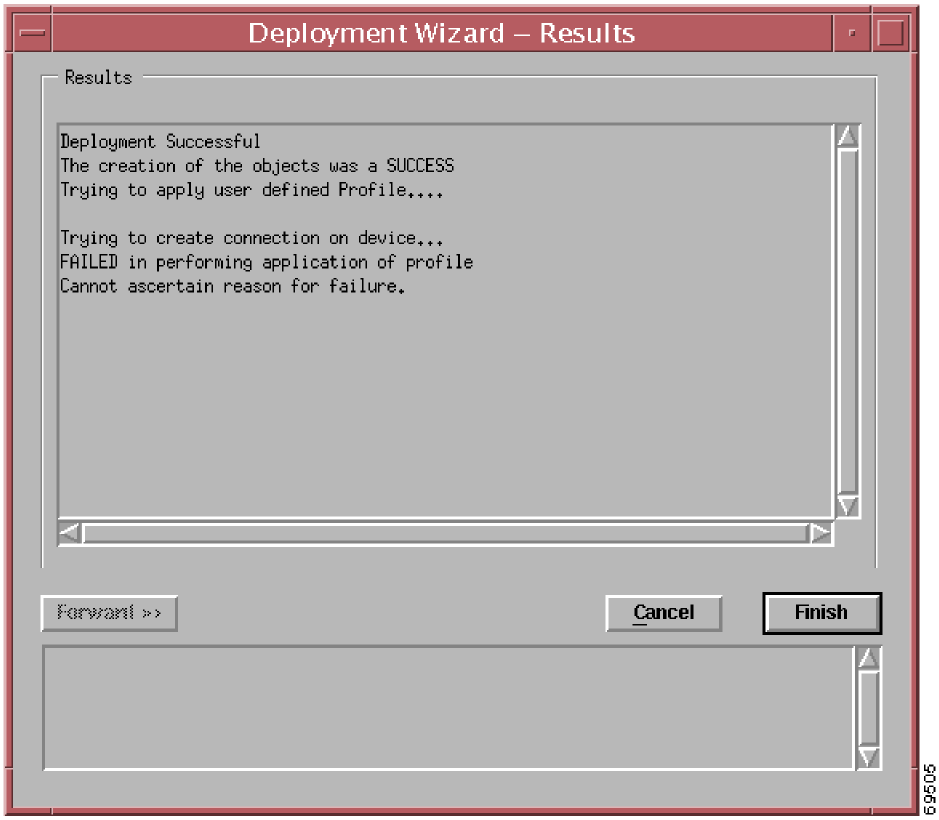
Figure 4-27 Deployment Wizard—Summary Window



Step 12 Click **Finish** to complete the deployment.

The Deployment Wizard—Results window opens and indicates whether the deployment was successful. (See Figure 4-28.)

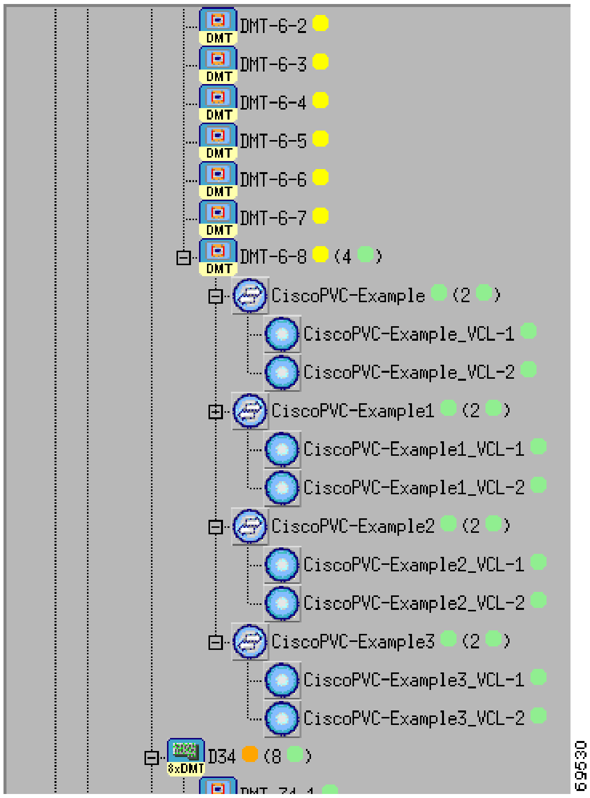
Figure 4-28 Deployment Wizard—Results Window



The Deployment Wizard—Summary window (see Figure 4-20) summarizes your deployment. In this example, the software failed to apply the profile. When you create a PVC or SPVC, the software also creates two virtual channel links (VCLs) that represent the two incoming and outgoing endpoints.

Note The number of objects that you enter in the Number of ciscoSPVC objects fields, is reflected on the left side of the Map Viewer window. For example, if you enter 8 in this field, 8 VCLs display below that interface. This example is shown in Figure 4-29.

Figure 4-29 Example of Deploying Multiple SPVC Objects



You can configure and view status and performance for these VCLs, which is described in the "Managing VCLs" section on page 4-39.

Note Deploying an ATM PVC or SPVC does not create the connection on the device. To create the actual connections, you must use the ATM QoS Profiles Management window and the ATM Connections Management window.

Applying an ATM QoS Profile to a PVC or SPVC

When you create a PVC or SPVC, you can specify the ATM QoS profile for that connection at deployment. When the DSLAM is synchronized, these connections and profiles are automatically uploaded.

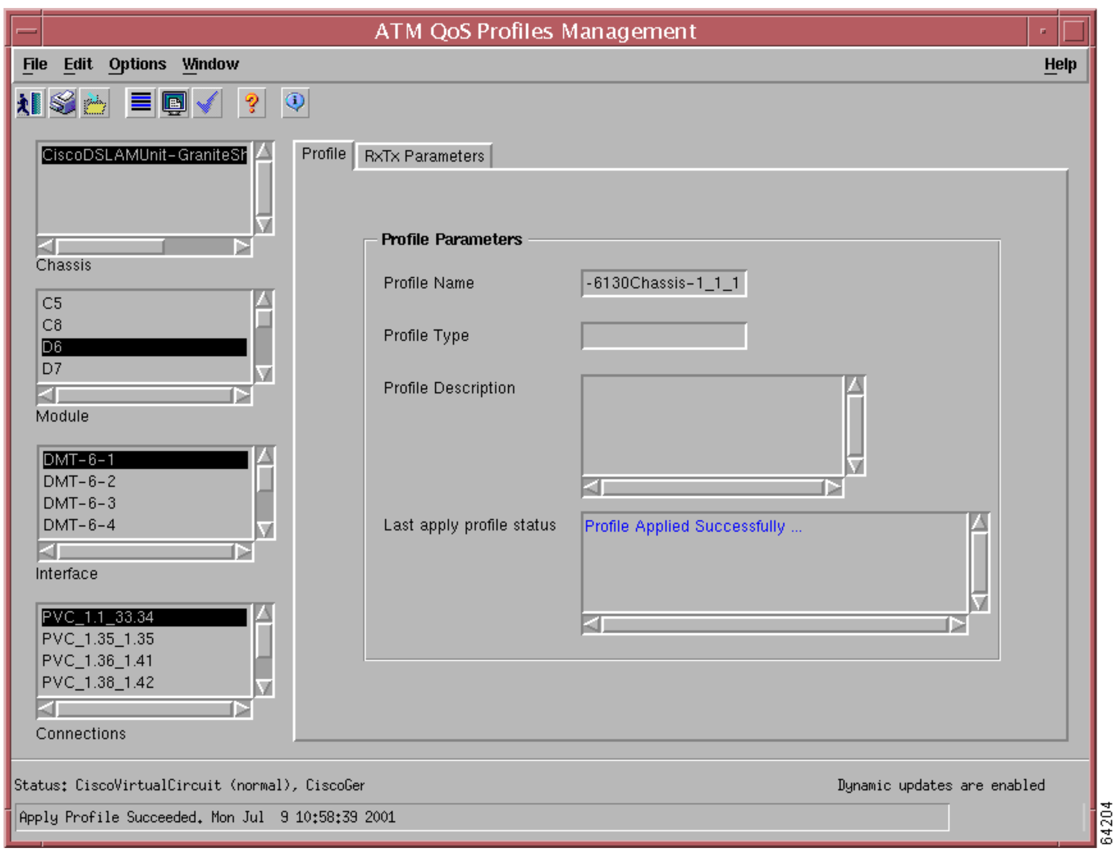
However, if for some reason the deployment is not completely successful, you can manually apply the ATM QoS profile to the PVC or SPVC. To apply an ATM QoS profile, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Component Managed view, right-click the chassis object to which you want to apply an ATM QoS profile.

Step 2 Choose **Cisco DSL Manager > Connection > Configuration > ATM** from the object menu.

The ATM Connection QoS Configuration window opens to the Profile tab opens. (See Figure 4-30.)

Figure 4-30 ATM Connection QoS Configuration Window—Profile Tab



Step 3 From the list box on the left side of the window, select the related chassis, card, interface, and connection (PVC or SPVC).

This connection should be the PVC or SPVC to which you want to apply the ATM QoS profile. Any current ATM QoS profile that is applied to the selected PVC or SPVC displays on the right side of the window.

Step 4 From the menu bar, choose **Edit > Apply Profile**.

A list of ATM QoS profiles displays to the right of the menu.

Step 5 Select the ATM QoS profile that you want to apply from the list.

After you apply the profile, a status line displays briefly in the lower left corner of the window that indicates whether CDM successfully applied the profile. The information for the selected new profile displays on the right side of the window.

Activating the PVC or SPVC Connection

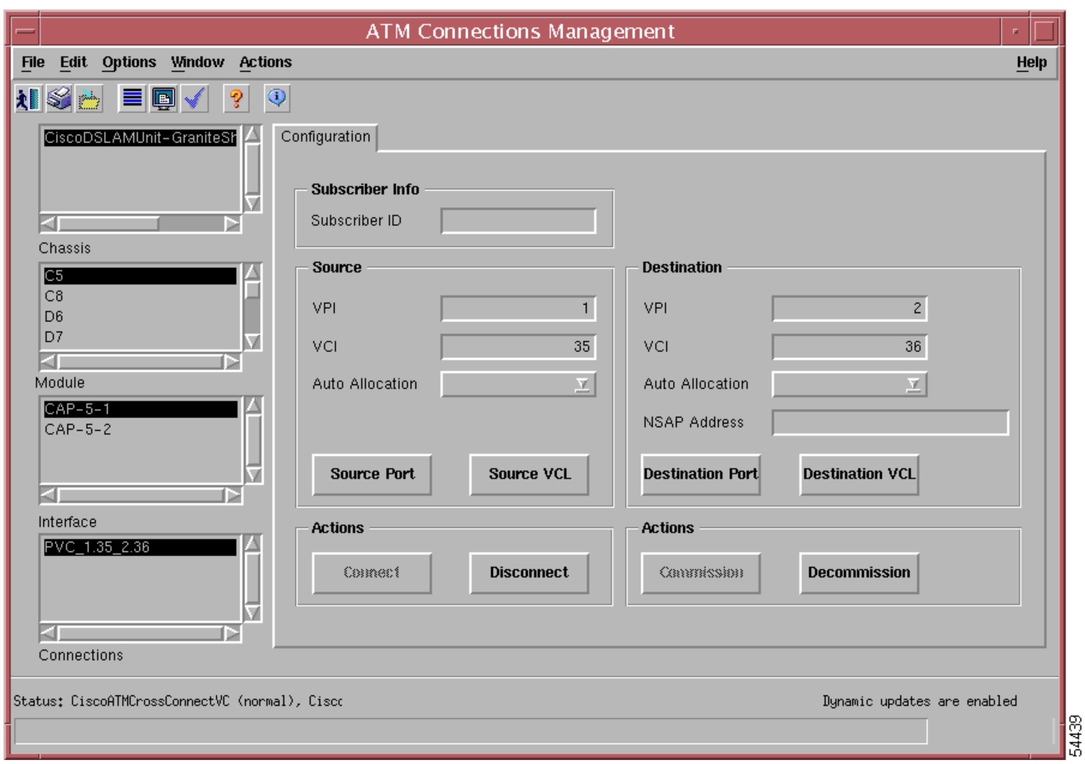
The instructions in this section are necessary only if a failure occurred when you deployed the PVC or SPVC. If a failure occurred after you created a PVC or SPVC in CDM and applied an ATM QoS profile to the PVC or SPVC, you can connect the PVC or SPVC on the device to activate the connection. Complete these steps to activate the connection:

Step 1 From the left side of the Map Viewer window, within the Component Managed view, right-click the chassis object for which you want to activate the PVC or SPVC connection.

Step 2 Choose **Cisco DSL Manager > Connection > Connection Management > ATM** from the object menu.

The ATM Connections Management window opens to the Configuration tab. (See Figure 4-31.)

Figure 4-31 ATM Connections Management Window



Step 3 From the left side of the window, select the related chassis, card, interface, and connection that you want to create.

Step 4 On the Configuration tab, enter the desired information in the Subscriber Info, Source, and Destination areas.

See Table 4-4 on page 4-38 for descriptions of the fields in this tab.

Note If you are creating an SPVC, the NSAP Address for the outgoing port also displays.

Step 5 Click **Connect** in the Action area.

You are prompted to confirm this action. Clicking the Connect button instructs CDM to create the subscriber connection on the device. The connection object changes to the Normal state.

Step 6 If you want to disconnect the subscriber connection, click **Disconnect**.

In the second Actions area, you can click the Decommission button, which suspends management of the connection. When you decommission a connection, alarms are no longer reported against this connection and performance polling is no longer performed on the connection.

Table 4-4 contains information about the parameters in the Subscriber Info, Source, and Destination areas of the Configuration Tab.

Table 4-4 ATM Connections Management—Configuration Tab Parameter Definitions

Parameter	Definition
Subscriber Info	
Subscriber ID	Enter the subscriber ID.
Source	
Source VPI	Enter the VPI value of the source VCL. For Cisco CPEs this value can be 1. For CPEs that are non-Cisco and for SPVCs, this value can be 32 to 4000. For PVCs, this value can be 0 to 355.
Source VCI	Enter the VCI value of the source VCL. For Cisco CPEs, this value can be 0 to 3. For CPEs that are non-Cisco and for SPVCs, it can be 1 to 1000. For PVCs, this value can be 32 to 16383.
Auto Allocation	Use the down arrow to select enable or disable. The source VPI and source VCI values are provided automatically if you click the **Source Port** and **Source VCL** buttons. The Source Port button displays the ATM Configuration window for the selected PVC or SPVC. The Source VCL button displays the VCL Configuration window for the selected PVC or SPVC. These buttons allow you to view or perform more detailed configuration on both VCLs.
Destination	
Destination VPI/Destination VCI	VPI and VCI values of the destination VCL. If you set the VPI value to 0 or 2 to 27, VCI can be 0 to 399. If you set the VPI value to 1, VCI can be 1 to 1599.

Table 4-4 ATM Connections Management—Configuration Tab Parameter Definitions (continued)

Parameter	Definition
Auto Allocation	The source VPI and source VCI values are provided automatically if you select the Auto Allocation button on each side (Source and Destination.)
NSAP Address	The ATM address that you must provide if you are configuring an SPVC with a non CEMF endpoint. When your configuration includes a subtended chassis, you must provide the NSAP address for the destination ATM end point of the connection. **Note** This field is only applicable to SPVCs, not PVCs. Clicking the Destination Port button displays the ATM Configuration window for the selected PVC or SPVC. Clicking the Destination VCL button displays the VCL Configuration window for the selected PVC or SPVC. Clicking these buttons allows you to view and perform more detailed configuration on both VCLs. See the "Managing VCLs" section on page 4-39 for more information about configuring VCLs.

Managing VCLs

This section includes the following topics:

When you create an ATM connection (PVC or SPVC), CDM automatically creates two Virtual Channel Links (VCLs). One VCL represents the source or incoming port, and the other VCL represents the destination or outgoing port. You can view or modify the configuration, performance, and status of VCLs through the VCL Management window.

Configuring a VCL

This section includes instructions for configuring an ATM VCL through the ATM VCL Configuration window and setting up Layer 3 configuration parameters in the ATM VCL Configuration window Layer 3 Configuration tab.

Using the ATM VCL Configuration Window—Configuration Tab

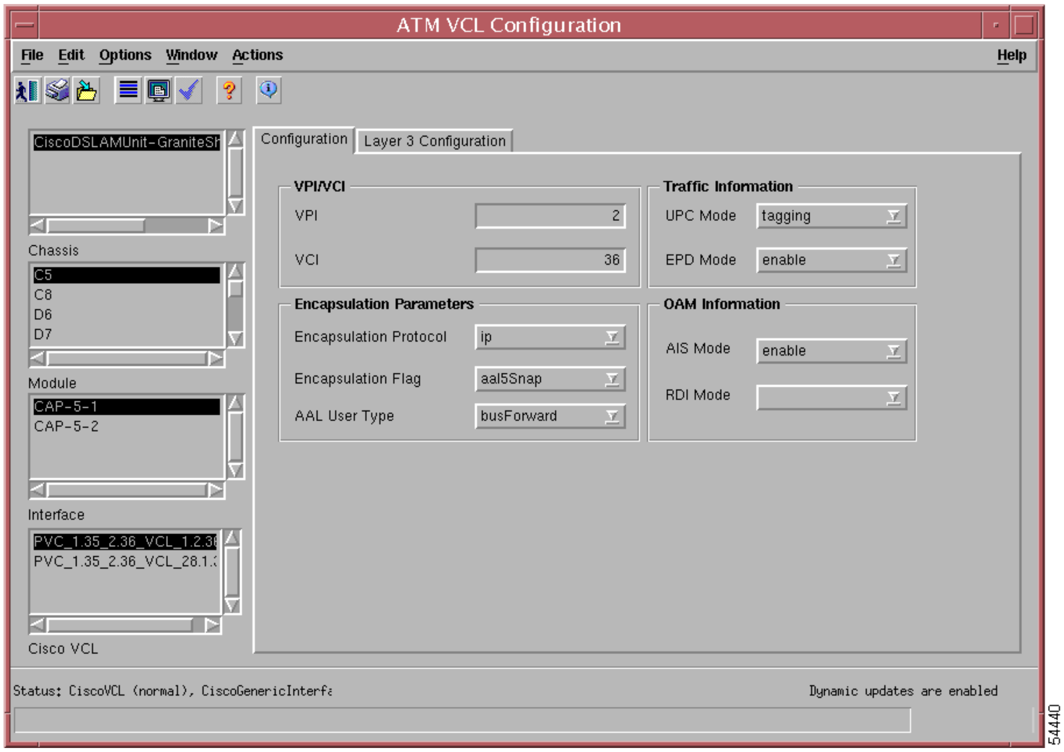
To configure an ATM VCL, open the VCL Management window as follows:

Step 1 In the Map Viewer window, within the Component Managed view, right-click the interface that has a PVC already created and for which you want to configure a VCL.

Step 2 Choose **Cisco DSL Manager> Connection > VCL Management > Config** from the object menu.

The ATM VCL Configuration window opens. (See Figure 4-32.)

Figure 4-32 ATM VCL Configuration Window—Configuration Tab



Step 3 Select a VCL from the list box on the left side of the window.

The Configuration tab contains four areas:

- VPI/VCI
- Traffic Information
- Encapsulation Parameters
- OAM Information

Configure the values for the VCL that you have selected in Step 5.

Step 4 The VPI/VCI area contains the following information (read only):

a. In the VPI field, VPI values display for either the source VCL or the destination VCL, depending upon the type of VCL that you select.

b. In the VCI field, the VCI values display for either the source VCL or the destination VCL, depending upon the type of VCL that you select.

Step 5 In the Traffic Information area, enter the following information:

a. In the UPC Mode field, use the down arrow to select **pass**, **tag**, **drop**, or **local shaping** for the Usage Parameter Control Mode on the established connection.

b. In the EPD Mode field, use the down arrow to select **enable** or **disable**, to enable or disable early packet discard at this specific connection.

Step 6 In the Encapsulation Parameters area, determine whether to set the following fields:

a. If the Encapsulation Flag is set to aal5Mux, use the down arrow in the Encapsulation Protocol field to specify the Protocol for the terminating VC; if the Encapsulation Flag is not set to aal5Mux, you do not need to set this parameter.

Valid choices include the following parameters:

- other
- ip
- xns
- appletalk
- clns
- decnet
- novell
- apollo
- vines

b. In the Encapsulation Flag field, use the down arrow to specify the encapsulation type for the terminating VC.

Valid choices include the following parameters. ATM Adaptation Layer 5 (AAL5) segments and reassembles data units up to 65,535 octets into ATM cell payloads. AAL5 is suited for variable bit rate traffic such as TCP/IP and signalling.

- aal5Snap—AAL5 subnetwork access protocol
- aal5Nlpid—AAL5 network layer protocol ID
- aal5FrNlpid—AAL5 frame relay network layer protocol ID (not used)
- aal5Mux—AAL5 multiprotocol over ATM
- aal34Smds—AAL3/4 switched multimegabit data service
- aalQsAal—Signalling AAL
- aal5Ilmi—AAL5 integrated local management interface
- aal5Lane—AAL5 LAN emulation
- aal5Pnni—AAL5 private network to network interface

c. If the Encapsulation flag field is set to aal5Lane, use the down arrow to set the AAL User Type parameter; if the Encapsulation Flag is not set to aal5Lane, you do not need to set this parameter.

Valid options include the following parameters:

- other
- boxConfigure—Shared Server/Client end of a Configure VCC
- busForward—BUS end of the Data Forward VCC
- busSend—BUS end of the Data Send VCC
- clientConfigure—LE Client end of the Configure Direct VCC
- clientData—One end of the Data Direct VCC
- clientDirect—LE Client end of the Control Direct VCC
- clientDistribute—LE Client end of the Control Distribute VCC

- clientForward—LE Client end of the Multicast Forward VCC
- clientSend—LE Client end of the Multicast Send VCC
- configure—Config Server end of any Configure VCC
- serverConfigure—LE Server end of the Configure VCC
- serverDirect—LE Server end of the Control Direct VCC
- serverDistribute—LE Server end of the Control Distribute VCC

Step 7 In the operation, administration, and maintenance (OAM) cell Information area, enter the following information:

a. In the AIS Mode field, use the down arrow to select **enable** or **disable**.

This field enables or disables the Enable Alarm Indication Signal OAM cell generation if the interface fails when cross-connecting virtual channel.

b. In the RDI Mode field, use the down arrow to select **enable** or **disable**.

This fields enables or disables the Enable Remote Defect Indication (RDI) OAM cell generation. In ATM, if the physical layer detects loss of signal or cell synchronization, RDI cells report a VPC/VCC failure. RDI cells are sent upstream by a VPC/VCC end point to notify the source VPC/VCC end point of the downstream failure.

Step 8 Click **Save** in the toolbar to save your configuration settings.

The configuration information for the selected VCL displays on the right side of the window. You can view or modify this information.

Description of the ATM VCL Configuration Window—Configuration Tab

Table 4-5 describes the fields in the ATM VCL Configuration Window Configuration tab.

Table 4-5 ATM VCL Configuration Window—Configuration Tab Field Definitions

Field	Definition
VPI/VCI	
VPI	Displays the VPI for the selected interface.
VCI	Displays the VCI for the selected interface.
Traffic Information	
UPC[1] Mode	Use the down arrow to select from the following choices. This field specifies cell traffic handling based on the guaranteed quality of service for a subscriber: • passing—Allows the cell to pass through • tagging—Tags the cell and allows it to go through; because the cell is tagged, it could get dropped later if the network is congested. • dropping—Drops the cell. • local shaping
EPD[2] Mode	Use the down arrow to enable or disable this mode.

Table 4-5 ATM VCL Configuration Window—Configuration Tab Field Definitions (continued)

Field	Definition
Encapsulation Parameters	
Encapsulation Protocol	Use the down arrow to specify the protocol if the encapsulation flag parameter is set to aal5Mux from the following choices: • other • ip • xns • appletalk • clns • decnet • novell • apollo • vines
Encapsulation Flag	Use the down arrow to set the encapsulation flag from the following choices: • aal5Snap—AAL5 subnetwork access protocol • aal5Nlpid—AAL5 network layer protocol ID • aal5FrNlpid—(not used) • aal5Mux—AAL5 multiprotocol over ATM • aal34Smds—AAL3/4 switched multimegabit data service • aalQsAal—Signalling AAL • aal5Ilmi—AAL5 integrated local management interface • aal5Lane—AAL5 LAN emulation • aal5Pnni—AAL5 private network to network interface

Table 4-5 ATM VCL Configuration Window—Configuration Tab Field Definitions (continued)

Field	Definition
Encapsulation Parameters	
Encapsulation Protocol	Use the down arrow to specify the protocol if the encapsulation flag parameter is set to aal5Mux from the following choices: • other • ip • xns • appletalk • clns • decnet • novell • apollo • vines
Encapsulation Flag	Use the down arrow to set the encapsulation flag from the following choices: • aal5Snap—AAL5 subnetwork access protocol • aal5Nlpid—AAL5 network layer protocol ID • aal5FrNlpid—(not used) • aal5Mux—AAL5 multiprotocol over ATM • aal34Smds—AAL3/4 switched multimegabit data service • aalQsAal—Signalling AAL • aal5Ilmi—AAL5 integrated local management interface • aal5Lane—AAL5 LAN emulation • aal5Pnni—AAL5 private network to network interface

Table 4-5 ATM VCL Configuration Window—Configuration Tab Field Definitions (continued)

Field	Definition
AAL[3] User Type	Use the down arrow to set the AAL user type parameter if the encapsulation flag is set to aal5Lane from the following choices: • other • boxConfigure—Shared Server/Client end of a Configure VCC • busForward—BUS[4] end of the Data Forward VCC • busSend—BUS end of the Data Send VCC • clientConfigure—LE[5] Client end of the Configure Direct VCC • clientData—One end of the Data Direct VCC • clientDirect—LE Client end of the Control Direct VCC • clientDistribute—LE Client end of the Control Distribute VCC • clientForward—LE Client end of the Multicast Forward VCC • clientSend—LE Client end of the Multicast Send VCC • configure—Config Server end of any Configure VCC • serverConfigure—LE Server end of the Configure VCC • serverDirect—LE Server end of the Control Direct VCC • serverDistribute—LE Server end of the Control Distribute VCC
OAM Information	
AIS[6] Mode	Use the down arrow to select enable or disable.
RDI[7] Mode	Use the down arrow to select enable or disable.

1. UPC = usage parameter control
2. EPD = early packet discard
3. AAL = ATM adaptation layer
4. BUS = broadcast and unknown server
5. LE = LAN emulation
6. AIS = alarm indication signal
7. RDI = remote defect indication

Description of the ATM VCL Configuration Management Window—Layer 3 Configuration Tab

The Layer 3 Configuration tab is not used in CDM.

Viewing ATM VCL Performance

You can start performance logging for a selected connection to gather performance data for that connection in the VCL Performance window. You can view this performance data by using the Performance menu or in the Performance Manager window.

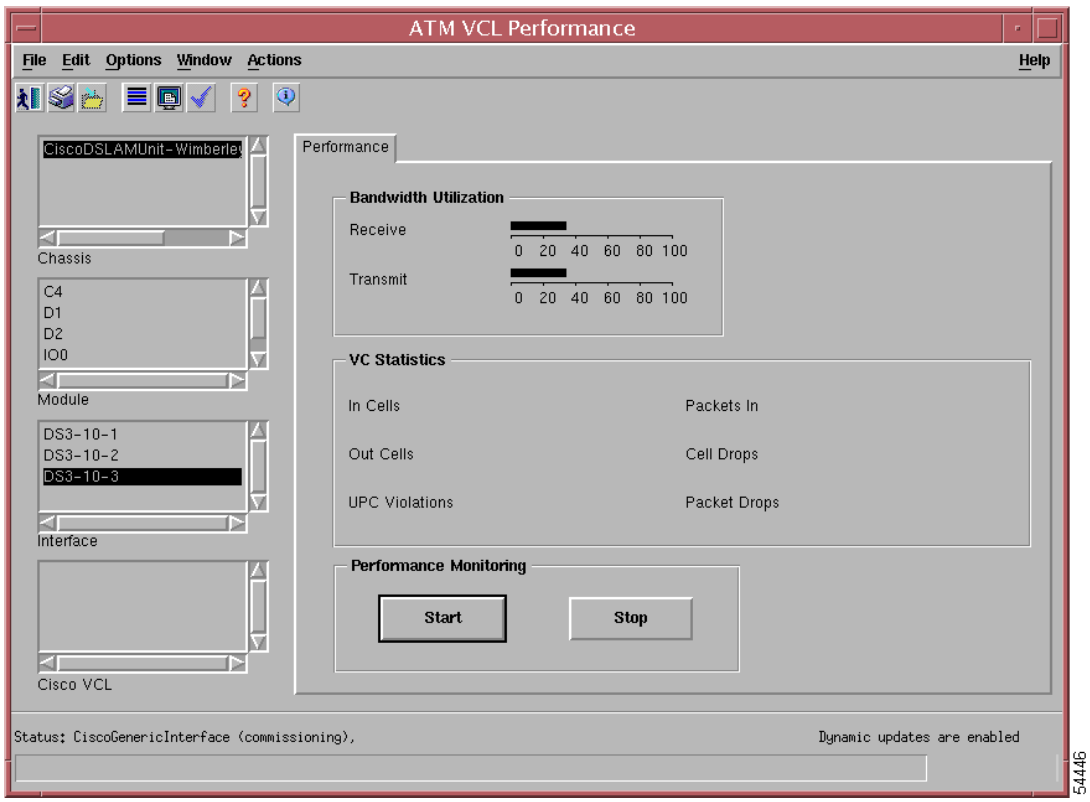
Complete the following steps to view ATM VCL performance:

Step 1 From the left side of the Map Viewer window, within the Component Managed view, right-click the chassis object whose VCL performance you want to monitor.

Step 2 Choose **Cisco DSL Manager > Connection > VCL Management > Performance** from the object menu.

The ATM VCL Performance window opens to the Performance tab. (See Figure 4-33.)

Figure 4-33 ATM VCL Performance Window



The chassis and module name that you selected are highlighted on the left.

Step 3 Click **Start** to begin performance polling on the selected VCL.

Step 4 Click **Yes** in the Yes/No dialog box to start performance polling.

The Action Report window opens and displays the status of this action. When polling is complete, the ATM VCL performance data for this chassis and module displays on the right side of the window.

The Performance tab contains three areas:

- Bandwidth Utilization
- VC Statistics
- Performance Monitoring

The fields in this tab are described in Table 4-6.

Table 4-6 ATM VCL Performance Window—Performance Tab Field Descriptions

Field	Description
Bandwidth Utilization	
Receive	Not used.
Transmit	Not used.
VC Statistics	
In Cells	Displays the total number of cells received on this VCL.
Out Cells	Displays the total number of cells transmitted on this VCL.
UPC[1] Violations	Displays the total number of UPC Violations on this VCL.
Packets In	Displays the total number of packets received on this VCL.
Cell Drops	Displays the total number of cells dropped on this VCL.
Packet Drops	Displays the total number of packets dropped on this VCL.
Performance Monitoring	
Start and Stop	Click the **Start** button to initiate performance monitoring on the selected VCL; click the **Stop** button to end performance monitoring. Performance monitoring collects and displays data on the object, either in the Performance windows or the Performance Manager. See Chapter 8, "Viewing Performance Data," for more information about monitoring performance.

1. UPC = usage parameter control

Viewing VCL Status

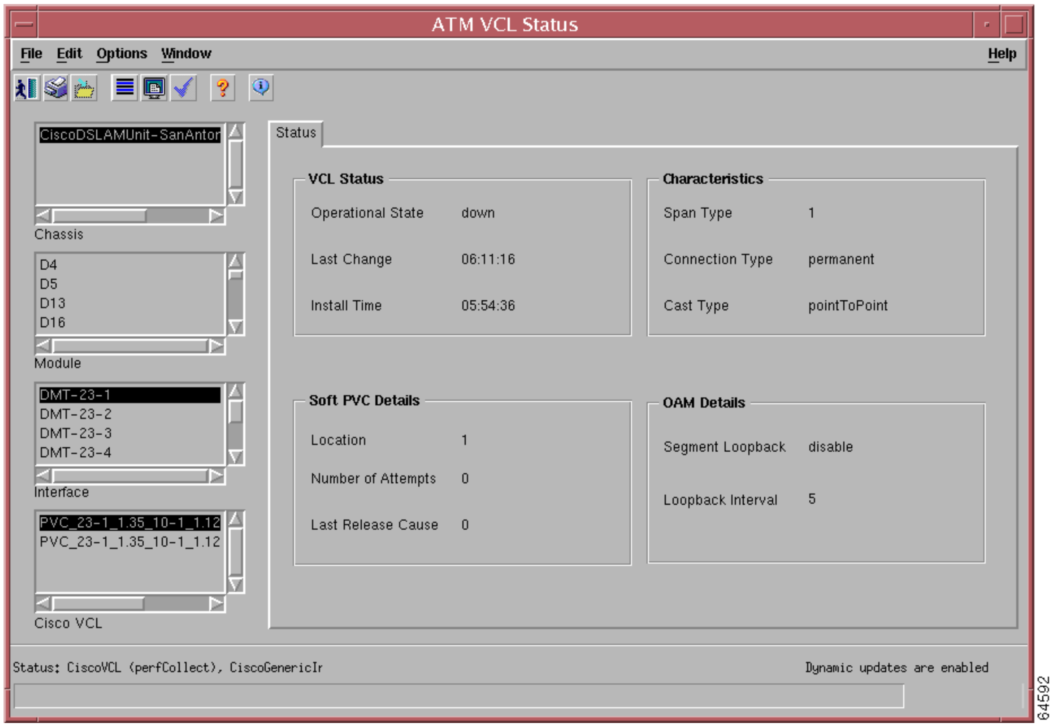
To view VCL status, follow these steps:

Step 1 From the left side of the Map Viewer window, within the Component Managed view, right-click the line card interface whose VCL status you want to view.

Step 2 Choose **Cisco DSL Manager > Connection > VCL Management > Status** from the object menu.

The ATM VCL Status window opens to the Status tab. (See Figure 4-34.)

Figure 4-34 ATM VCL Status Window



Step 3 The line card you selected is highlighted on the left, or from the list box on the left side of the window, select a VCL.

The status information for the selected VCL displays on the right.

The Status tab contains four areas:

- VCL Status
- Characteristics
- Soft PVC Details
- OAM Details

Table 4-7 provides descriptions of the fields in this window.

Table 4-7 ATM VCL Status Window—Status Tab Field Descriptions

Field	Description
VCL Status	
Operational State	Displays the status of the VCL connection.
Last Change	Displays the time elapsed since the last status change.
Install Time	Displays the time elapsed since the last installation.

Table 4-7 ATM VCL Status Window—Status Tab Field Descriptions (continued)

Field	Description
Characteristics	
Span Type	Displays the VCL span type.
Connection Type	Displays the virtual connection configuration type.
Cast Type	Displays the virtual connection cast type.
Soft PVC Details	
Location	Indicates the calling or called side of a SPVC.
Number of Attempts	Indicates the number of attempts made to install this SPVC.
Last Release Cause	Indicates the cause of the last connection release.
OAM Details	
Segment Loopback	Indicates whether the segment loopback is enabled or disabled on the virtual channel selected.
Loopback Interval	Indicates the frequency with which the OAM loopback cells are generated.

Manually Uploading ATM QoS Profiles

CDM automatically synchronizes connection information (that is, PVC and SPVCs) between the DSLAM and CDM. This synchronization process occurs at regular intervals; the default is every 30 minutes. However an operator can manually force an upload of connection information.

When you upload existing ATM connections and ATM QoS profiles, CDM discovers any existing ATM connections and places them into the Normal state. You can then begin automatically managing the subscribers associated with these connections. CDM uploads ATM QoS profiles and PVCs or SPVCs and their associated connection parameters (VPIs and VCIs) to the correct interfaces; you can then view and adjust them in the CDM GUI.

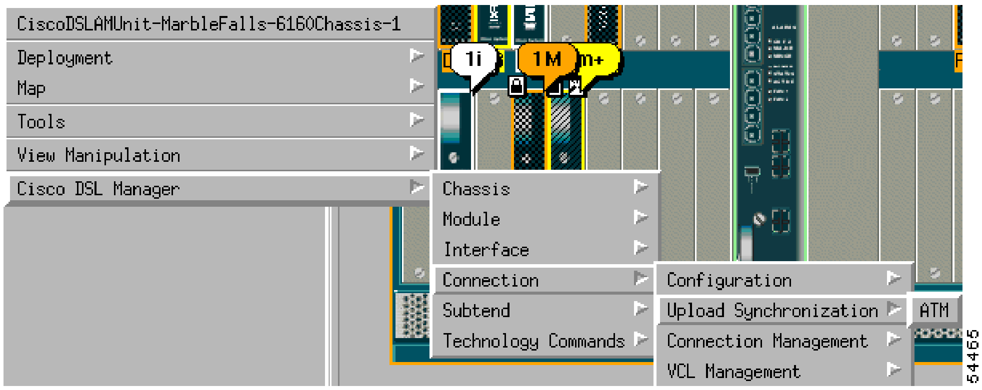
Note CDM uploads PVC and SPVC information based on the connection synchronization policy that you have selected. See the "Polling the Chassis and Setting the Connection Synchronization Policy" section on page 4-1 for more information.

If your deployment of PVCs or SPVCs and associated ATM QoS profiles fails, you can upload them manually by completing the following steps:

Step 1 In the Map Viewer window, within the Physical view, right-click a chassis object to access the object menu.

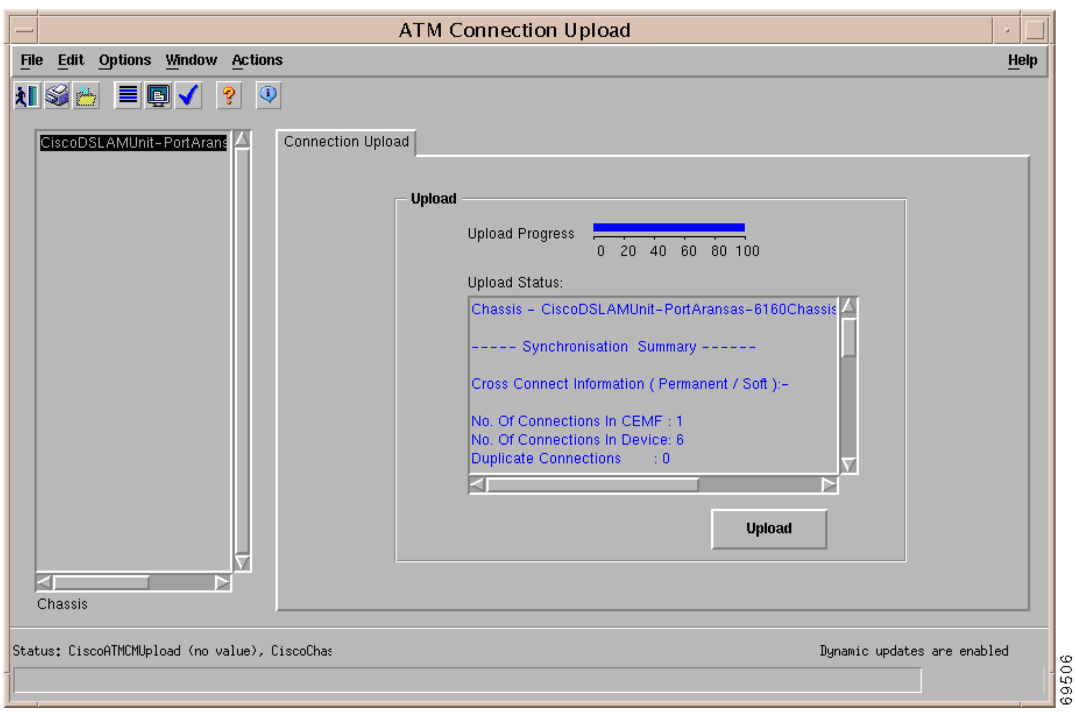
Step 2 Choose **Cisco DSL Manager > Connection > Upload Synchronization > ATM**. (See Figure 4-35.)

Figure 4-35 Choosing Upload Synchronization from the Object Menu



The ATM Connection Upload window opens. (See Figure 4-36.)

Figure 4-36 ATM Connection Upload Window



The name of the chassis that you selected is highlighted in the list box on the left side of the window.

The names of uploaded ATM connections and ATM QoS profiles are based on the following formats:

- ATM connections—PVC_(*index of incoming port.VPI value.VCI value.index of outgoing port.VPI value.VCI value*)
- ATM QoS profiles—QoSProfile_(assigned number)

Step 3 Click **Upload**.

All ATM connections and ATM QoS profiles that are currently configured on the selected device are uploaded into CDM. The way you configure the connection synchronization policy determines which PVC and SPVC connections CDM uploads. See the "Polling the Chassis and Setting the Connection Synchronization Policy" section on page 4-1 for more information about how to configure the connection synchronization policy.

Using Inverse Multiplexing over ATM on Cisco 6015, 6160, and 6260 DSLAMs

This section is applicable to Cisco 6015, 6160, and 6260 DSLAMs.

You can use inverse multiplexing over ATM (IMA) to join together several slower speed links to create a virtual high-speed link. The following sections include an overview of IMA and how to move IMA links in CDM:

Overview of IMA

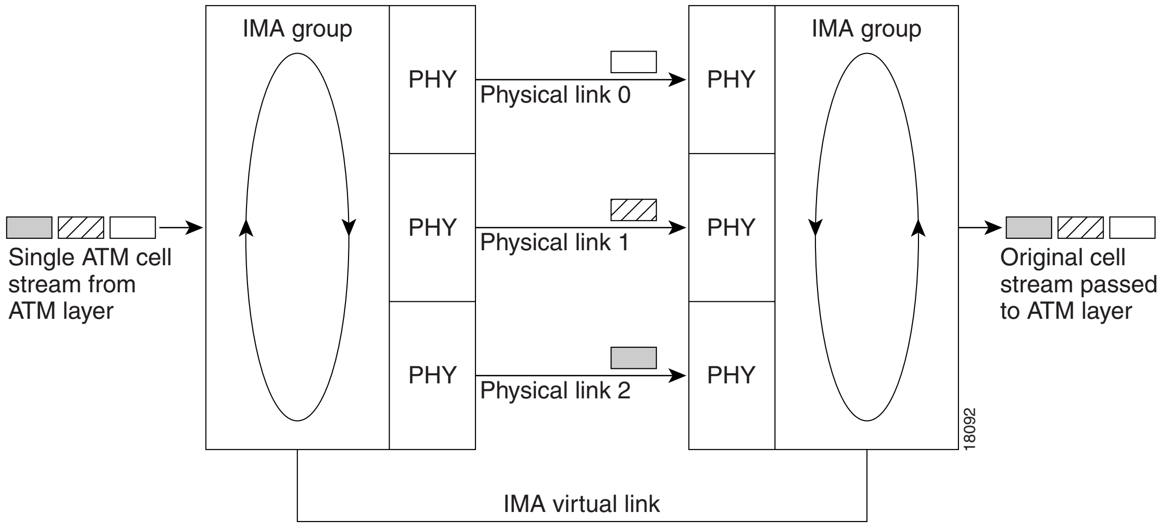
IMA provides access to ATM networks by combining the bandwidth of multiple DS1/E1 links into groups that collectively provide higher intermediate rates. In CDM, an IMA group can have up to 4 T1 links, and each link provides 1.544 Mbps.

IMA breaks up the ATM cell stream and distributes the cells over the multiple physical links of an IMA group, and then recombines the cells into a single stream at the other end of the connection. The ATM cells are distributed in a round robin fashion over the physical links of the IMA group, demultiplexed at the receiving IMA group, and passed in their original form to the ATM layer (see Figure 4-37). Using the multiple links of an IMA group increases the logical link bandwidth to approximately the sum of the individual link rates.

IMA requires a minimum of two commissioned chassis. CDM automatically provides four IMA groups to each chassis upon the completion of the commissioning process. You can use these IMA groups to group individual IMA links.

Note If you choose to assign IMA links to IMA groups, each group must be assigned the minimum number of links as configured in IOS. The default value is one link per group.

Figure 4-37 Inverse Multiplexing and Demultiplexing of ATM Cells Through IMA Groups



The T1 and E1 IMA port adapters have eight ports. You can use the eight ports on the T1 and E1 IMA port adapters as independent ATM links or in the IMA mode. Some examples of combinations include:

- Four IMA groups
- Three IMA groups and one independent ATM link
- Two IMA groups and two independent ATM links
- One IMA group and three independent ATM links
- No IMA group and four independent ATM links

The T1 (1.544 Mbps) and E1 (2.048 Mbps) IMA port adapters provide trunk connectivity and are used for intercampus or wide-area links. The T1 and E1 IMA port adapters support unshielded twisted-pair connectors.

Configuring IMA Groups

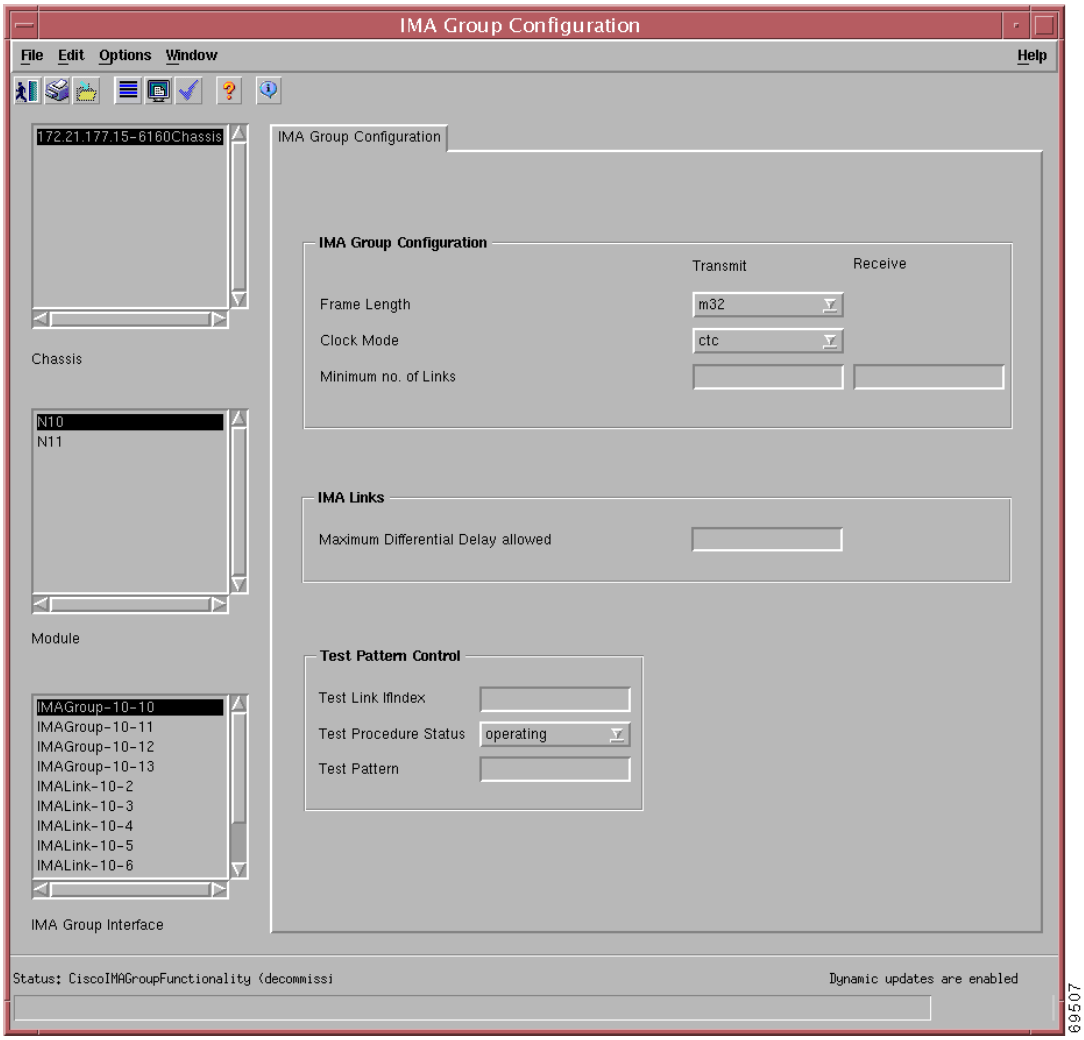
To configure IMA groups, complete the following steps:

Step 1 From the left side of the Map Viewer window, from within the Physical or IMA hierarchy view, right-click the NI card icon for the IMA group whose configuration you want to edit.

Step 2 Choose **Cisco DSL Manager > Interface > Configuration > IMA Configuration** from the object menu.

The IMA Group Configuration window opens. (See Figure 4-38.)

Figure 4-38 IMA Group Configuration Window



The left side list box displays the IMA group whose configuration you want to change.

Step 3 Edit the values in this window as needed.

Note The fields in this window are described in Table 4-8.

This window contains the following four areas:

- IMA Group Details
- IMA Group Configuration
- IMA Links
- Test Pattern Control

Table 4-8 IMA Group Configuration Window

Field	Description
IMA Group Details	
Symmetry	Displays the results of symmetric mode adjustment during IMA group start up.
Transit IMA ID	Displays the IMA link ID.
ICP[1]	Displays the current values for the following fields: • Alpha Value • Beta Value • Gamma Value
IMA Group Configuration	
Frame Length	Use the down arrow to select the transmit frame length from one of the following choices: • m32 • m64 • m128 • m256
Clock Mode	Use the down arrow to select the transmit clock mode. • cfc—common transmit clock • itc—independent transmit clock
Minimum no. of Links	Enter the minimum number of transmit and receive links that are required to be active for the IMA group to be in the operational state. Valid choices range from 1 to 32.
IMA Links	
Maximum Differential Delay allowed	Enter the maximum number of milliseconds of differential delay among the links that will be tolerated on this interface. The default value is 25.
Test Pattern Control	
Test Link ifindex[2]	Enter the value to designate an interface as the test link for use in the Test Pattern Procedure. The distinguished value of zero specifies that the implementation may choose the Test Link, in which case the implementation may also choose the value of 'imaGroupTestPattern'. The value zero may also be used if no link has yet been added to the group. **Note** This value is not the same as the Tx LID[3] value, but instead either identifies the ifIndex value of the test link to be used by the Test Pattern Procedure (that is, the link whose LID value is inserted in the Tx LID field of the transmitted ICP cells), or identifies that the implementation may choose the test link (if the value is zero). The default value for this field is 0.

Table 4-8 IMA Group Configuration Window (continued)

Field	Description
Test Procedure Status	Use the down arrow to select disabled, operating, or linkFail.
Test Pattern	Enter the test pattern to invoke a test pattern object. Test pattern objects are implemented if the IMA implements the test pattern procedure. In this case, all test pattern procedure-related objects must be implemented. Specifically, these objects include: • imaGroupTestLinkIfIndex • imaGroupTestPattern • imaGroupTestProcStatus • imaLinkRxTestPattern • imaLinkTestProcStatus

1. ICP = intelligent cell processing
2. ifindex = interface index
3. LID = link ID

Configuring Subtend Configurations

This chapter describes how to set up subtend configurations and how to set child DSLAM subscriber PVCs. Using subtend configurations allows you to use one ATM backbone for multiple Cisco DSLAMs.

This chapter includes the following sections:

Overview of Subtend Configurations

Using subtend configurations is a DSLAM feature that reduces the cost per subscriber by amortizing the expense of the network interface module and the edge-switch interface connection over a large number of subscribers. Subtend configurations provide the following advantages:

- Services and aggregates the data from one or more remotely located Cisco DSLAM into a host Cisco DSLAM. This configuration takes advantage of the data network interface on the host Cisco DSLAM.
- Reduces the number of ATM edge-switch interfaces that are required to terminate the Cisco DSLAM.

CDM subtend configurations support the following topology configurations:

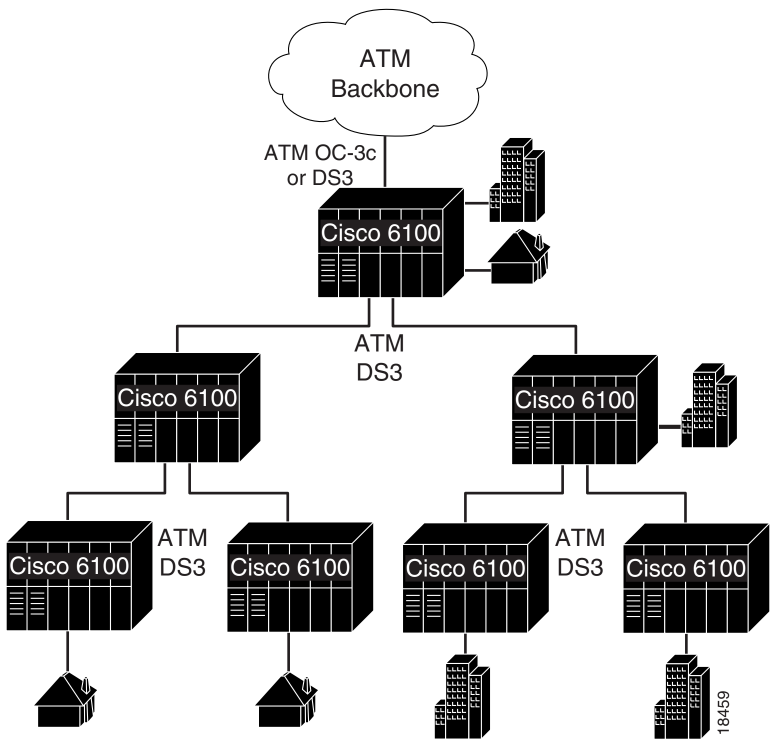
- Tree
- Daisy chain
- Star

CDM subtend configurations supports the following DSLAM interconnections, where the host chassis is called the parent, and the subtended chassis is called the child:

- NI-2 as parent with NI-2 as child
- NI-2 as parent with NI-1 as child
- NI-1 as parent with NI-1 as child

Figure 5-1 illustrates the connections of a subtend DSLAM configuration in a tree topology with six child systems. The example in this illustration uses Cisco 6100 DSLAMs but applies to all Cisco DSLAM chassis types.

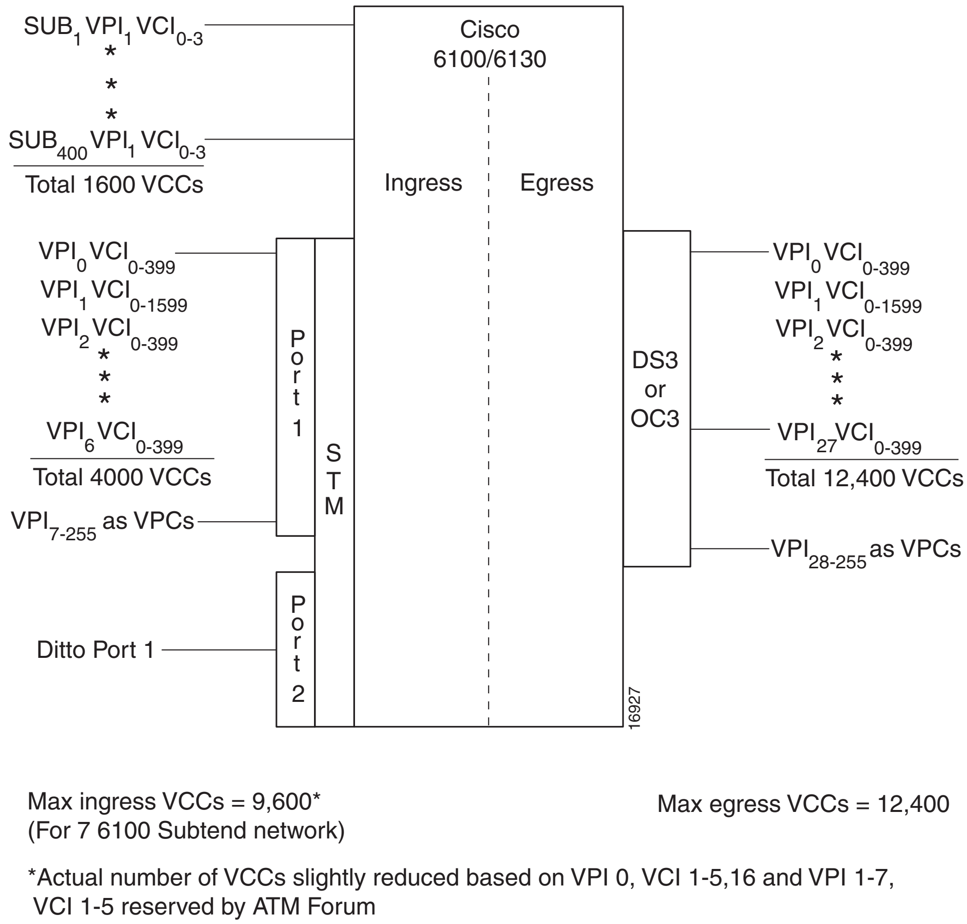
Figure 5-1 Subtend Connections



Note The same WAN technology must be used between a parent DSLAM and its subtended chassis (for example OC-3 to OC-3 or DS3 to DS3, single mode to single mode, and multimode to multimode), and all chassis must be physically connected. In this illustration, the parent DSLAM is using DS3 technology, but you can also set up a subtend configuration using OC-3 technology. In that case, the parent DSLAM also uses OC-3 technology.

Figure 5-2 shows valid address ranges for each DSLAM. The example in this illustration uses Cisco 6100/6130 DSLAMs, but applies to all Cisco DSLAM chassis types.

Figure 5-2 Valid ATM Connection Space



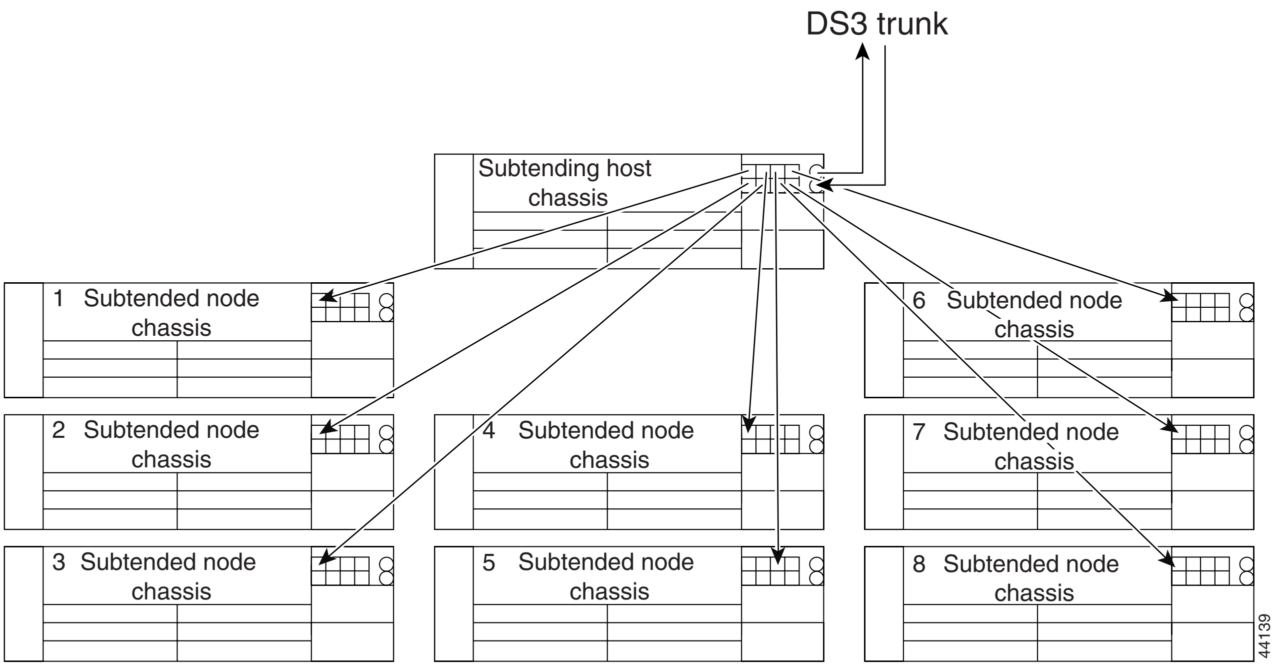
Guidelines for Configuring a Subtend System

The following guidelines apply to setting up a subtend configuration:

- Before you use CDM to manage a subtend system, you must set up the physical subtend configuration, and you must have a telnet session on a DSLAM to provide for IOS configurations.
- You can subtend several Cisco DSLAMs to one parent host Cisco DSLAM that is connected to the ATM network backbone (which is illustrated in Figure 5-1). The number of DSLAMS that one host or parent DSLAM can subtend, based on the type of topology, is as follows:
  - Tree topology—6 subtended DSLAMs (children)
  - Daisy chain topology—13 subtended DSLAMS (children)
  - Star topology—8 subtended DSLAMS (children)

Figure 5-3 shows an example of a star topology using a Cisco 6015 DSLAM; the configuration of this topology applies to all DSLAM chassis types.

Figure 5-3 Subtended Network—Star Topology



Note The DS3 interface is designated as the trunk in a subtended network configuration. Ask your network architect or Cisco customer service representative for examples of other subtend topology configurations.

- Use standard Cisco DSLAM network interface modules on the subtended DSLAM for interconnection to the host node.
- Subtend as many as 8 chassis to support up to 2800 subscribers per network connection.
- The Cisco DSLAM can support up to 9000 VCCs. The total number depends on the amount of system-controller and network-interface RAM that the resident software application requires.
- Cisco recommends a maximum of 1500 VCCs within the valid address space. Software limits might not be built in because of the temporary nature of this ceiling.
- You must conduct data path tests between your Cisco DSLAM and far-end equipment.
- Use these guidelines for configuring VPIs and VCIs for NI-2:

```
modem port <--> trunk
    modem port: VPI = 0-255; VCI = 0-255
    trunk port: VPI = 0-255; VCI = 32-16383
trunk <--> subtend port
    trunk port: VPI = 0-255; VCI = 32-16383
    subtend port: VPI = 0-255; VCI = 32-16383
```

- Use these guidelines for configuring VPIs and VCIs for NI-1:

```
Subscriber side:
    VPI = 1; VCI = 0-3.
Subtend Port:
    VPI = 0-6; VCI = 0-399 (0-1599 for VPI=1)
Network side:
    VPI=0-27; VCI=0-399 (0-1599 for VPI=1)
```

For example, if using only NI-1 nodes, the following example applies (approximately)

```
Source: VPI = 1 VCI = 0 - 3
Destination: VPI = 0 - 6 VCI = 0 - 399
```

Suppose you have connections like this:

```
A <- B <- C
    A is at top
    B is subtended to A
    C is subtended to B
```

When you provide VPI/VCI value pairs for example, S=src & D=Dst), then three PVCs are created in the three nodes, as follows:

```
1. S <-> D in C
2. D <-> D in B
3. D <-> D in A
```

Setting the DSLAM IOS Password

Before you configure a subtend system, you must set the IOS passwords so that CDM can create a PVC and discover the subtend topology. You only need to do this procedure if you use autodiscovery when you deploy the DSLAMs.

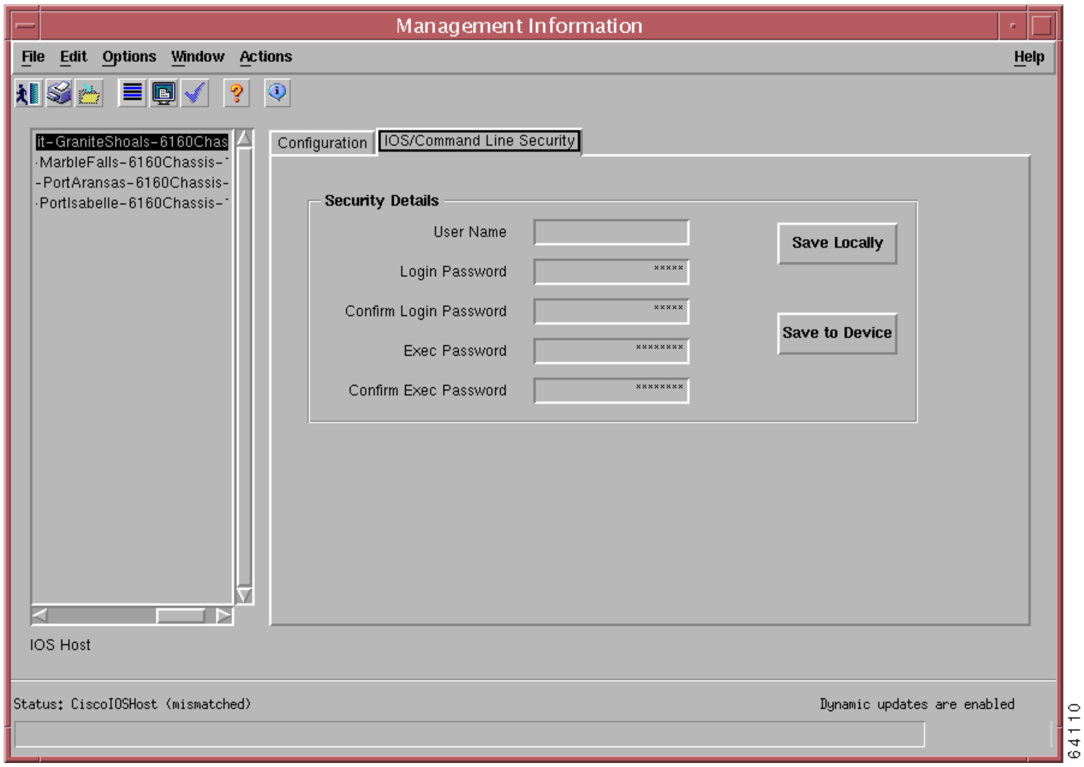
Complete the following steps to set the IOS passwords.

Step 1 From the left side of the Map Viewer window within the Physical view, right-click the chassis for which you want to set up a subtend configuration to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > IOS Settings**.

The Management Information window opens. (See Figure 5-4.)

Figure 5-4 Management Information Window—IOS/Command Line Security Tab



Step 3 In the IOS Host object list, select the DSLAM chassis that you want to configure as a parent host.

Step 4 Click the **IOS/Command Line Security** tab.

Step 5 In the Login Password field, enter the password that you will use to login to the DSLAM, for example, via Telnet.

Step 6 In the Confirm Login Password field, enter the login password again.

Step 7 In the Exec Password field, enter the password that you will use after the enable command.

Step 8 In the Confirm Exec Password field, enter the executive password again.

Step 9 Click **Save Locally**.

Preparing IOS Configurations

This section includes the following topics:

- Creating a Child DSLAM Using Telnet, page 5-7
- Connecting the Children DSLAMs, page 5-8

When you set up an ATM subtend configuration through CDM, you must first use the IOS CLI to prepare each subtended DSLAM chassis to be configured by CDM. Then use CDM to connect all the DSLAMs in the subtend configuration.

Before you can connect any of the DSLAMS, you need to determine which connections will be used as the trunk lines for both the parent DSLAM and each of its children. After you have defined these trunk lines for every DSLAM in the subtend topology, use the CDM Subtend Configuration window to connect the DSLAM. CDM can only connect the DSLAM; CDM does not designate which IMA groups will use the trunk in each DSLAM.

The following sections provide instructions to complete these tasks.

Note You must designate either an IMA link or IMA group as the trunk for each child in the topology. You use IOS to disable the DS3 line for each child; therefore you should not designate a DS3 or OC-3 connection as the trunk for a child DSLAM. The IMA links between DSLAMs serve as the connections. You can designate a DS3 or an OC-3 connection as a trunk only for a parent DSLAM.

The following sections provide instructions to complete these tasks.

Note You can also use the IOS CLI neighbor activate command to determine the IP address of DSLAMS that are in parent and children relationships. Refer to the *Command Reference for Cisco DSLAMs with NI-2* guide for information on using the neighbor commands.

Creating a Child DSLAM Using Telnet

This section describes how to use a telnet session to create a child DSLAM.

Note Before you create any children, be sure that the hardware is physically connected according to the desired topology.

To create a child DSLAM chassis using a Telnet session from CDM, complete the following steps:

Step 1 From the left side of the Map Viewer window, right-click the chassis name that you want to configure as the child.

The icon that represents that DSLAM displays on the right side of the Map Viewer window.

Step 2 Right-click the chassis icon to access the object menu.

Step 3 Choose **Technology Specific Tools > Initiate Telnet Session**.

A Telnet window opens.

Step 4 Enter your password.

Step 5 Enter the exec password.

Step 6 At the prompt, enter **en** to gain access to the topology network.

Step 7 Enter the IOS security password.

Step 8 Disable the DS3 connection (atm 0/1) for the child chassis by entering the following commands:

config t
int atm 0/0
shut

Step 9 Deactivate the T1 (atm 0/2 to 0/9) connection that you want to designate as the trunk for this child by entering the following commands:

config t
int atm 0/*x*

Where *x* is the interface number of the T1 line (0/2 to 0/9). See Figure 5-5 for a diagram of Cisco 6015 T1 line interface addresses.

shut
end

Figure 5-5 interface Addresses for Cisco 6015 Chassis T1 Lines

ATM 0/2	ATM 0/3	ATM 0/4	ATM 0/5
ATM 0/6	ATM 0/7	ATM 0/8	ATM 0/9

50242

Step 10 Designate the selected T1 connection as the trunk for the child by entering the following commands:

configure terminal
atm ni2-switch trunk ATM0/*x*

Where *x* is the interface number of the T1 line (0/2 to 0/9).

end

Step 11 Reactivate the T1 connection by entering the following commands:

config t
int atm 0/*x*

Where *x* is the interface number of the T1 line (0/2 to 0/9).

no shut

Step 12 Write the configuration to NVRAM.

Step 13 Repeat Step 8 through Step 12 for each child chassis.

Step 14 To end the telnet session, enter the following command:

exit

When you have created all children chassis, continue with the "Connecting the Children DSLAMs" section on page 5-8. Also, see the "Using Inverse Multiplexing over ATM on Cisco 6015, 6160, and 6260 DSLAMs" section on page 4-51 for information about setting up the IMA links.

Connecting the Children DSLAMs

After you have established the trunk lines for each child, use CDM to connect each child to the parent DSLAM. As you connect each child to the parent, an icon that represents that child displays in the Map Viewer window.

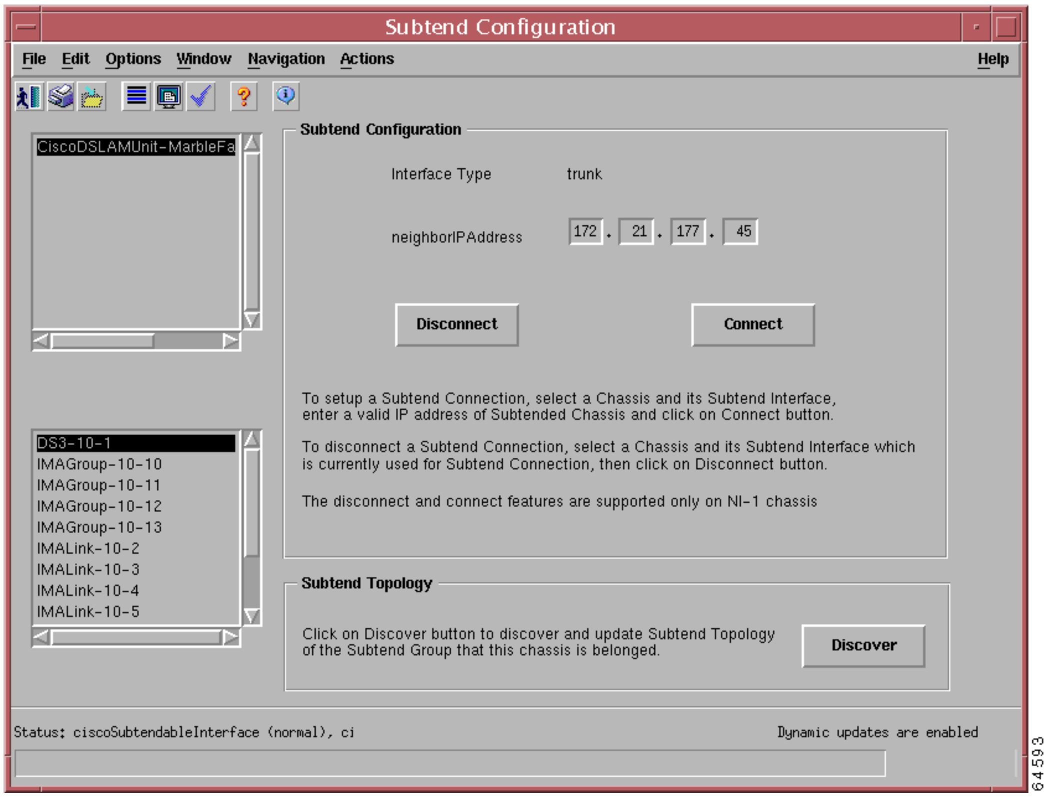
To connect a child to the parent DSLAM, complete the following steps:

Step 1 From the left side of the Map Viewer window within the Subtend view, right-click the parent DSLAM to which you want to connect a child.

Step 2 Choose **Cisco DSL Manager > Subtend > Subtend Configuration** from the object menu.

The Subtend Configuration window opens. (See Figure 5-6.)

Figure 5-6 Subtend Configuration Window



The DSLAM chassis that you have chosen to be the parent displays in the top list box on the left side of the window. After CDM discovers the subtend interfaces that you set up in the "Creating a Child DSLAM Using Telnet" section on page 5-7 (when you click **Discover** in Step 3 below), the interfaces display in the lower list box on the left.

Note Do not manually enter an IP address in the neighborIPAddress fields. CDM provides the IP address of each child as it discovers and connects each child.

Step 3 Click **Discover**.

CDM discovers all the children (the subtend interfaces that you set up in the "Creating a Child DSLAM Using Telnet" section on page 5-7) and displays them in the lower list box on the left side of the window.

Step 4 Click the interface of the child DSLAM in the lower list box that you want CDM to connect to the parent DSLAM.

Step 5 Click **Discover**; or, for NI-1 configurations, click **Connect**.

The IP address of the child chassis displays in the neighborIPAddress field.

Step 6 Repeat Step 4 and Step 5 for each child chassis that you want to connect to the parent chassis.

Deploying a Parent DSLAM

You deploy a parent Cisco DSLAM by using the same basic procedure that you use to deploy any other chassis. You also set up profiles and preprovision the line cards as you would in any DSLAM. This section summarizes the steps for deploying a parent DSLAM, as follows:

Step 1 From the left side of the Map Viewer window, under the Physical Site view, right-click to access the object menu.

Step 2 Choose **Deployment > Deploy Cisco DSLAM**.

The Deployment Wizard window opens.

Step 3 Follow the instructions in the series of Deployment Wizard windows to deploy the parent DSLAM.

> **Note** See the "Manually Deploying a Cisco DSLAM Chassis" section on page 2-13 for instructions to deploy a DSLAM.

The newly deployed parent chassis displays under the site to which you deployed it as CiscoDSLAMUnit-[Name of TopShelf DSLAM Chassis]. Next you must commission the newly deployed parent chassis, as follows:

Step 4 Right-click CiscoDSLAMUnit-[Name of TopShelf DSLAM Chassis] to access the object menu.

Step 5 Choose **Cisco DSL Manager > Chassis > Configuration**.

The Chassis Configuration window opens.

Step 6 If more than one chassis is listed in the list box on the left of this window, highlight the name of the chassis you want to commission by clicking it.

Step 7 Click **Commission** at the bottom of the window to commission the newly deployed parent chassis.

Step 8 After CDM successfully commissions the parent DSLAM chassis, you can close this window.

You can see the populated parent DSLAM on the right side of the Map Viewer window. Next you must update the parent DSLAM so that it recognizes the children DSLAM chassis.

Using CDM to Configure a Subtend System

CDM supports the following subtend management capabilities:

- You can connect two DSLAMs into a subtend configuration.
- You can disconnect two DSLAMs from a subtend configuration.
- CDM discovers the topology. For a given DSLAM, CDM discovers the entire topology of all DSLAMs that are connected in a subtend relationship. (See the "Connecting the Children DSLAMs" section on page 5-8.)
- You can create a subtend PVC.
- You can delete a subtend PVC.

Discovering the System Topology of a Subtend Configuration

This section includes instructions for updating and discovering subtend topology and applies only to a configuration in which an NI-1 subtends an NI-2.

Note The parent DSLAM and any children DSLAMS, must be physically connected before you update the topology.

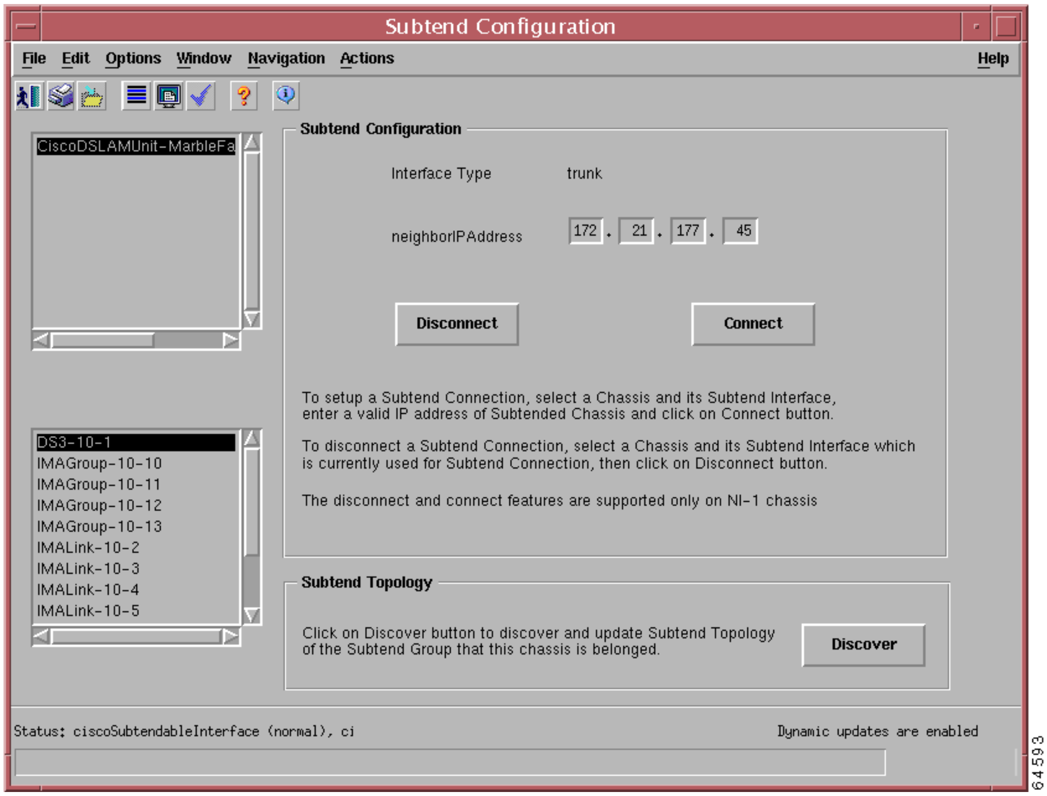
Complete the following steps to update the topology for a selected subtend DSLAM configuration.

Step 1 From the left side of the Map Viewer window, within the Component Managed view, right-click the CiscoDSLAMUnit [name of parent chassis] that you have deployed to access the object menu.

Step 2 Choose **Cisco DSL Subtend Manager > Subtend > Subtend Configuration**.

The Subtend Configuration window opens. (See Figure 5-7.)

Figure 5-7 Subtend Configuration Window



Step 3 From the list box of chassis on the left side of the window, click the chassis whose topology you want to update.

Step 4 Click **Discover** to initiate discovery of all DSLAMS that are connected to the DSLAM that you selected from the list box.

Step 5 From the list box on the left of network interfaces, click the trunk interface.

In the Subtend Configuration area, the Interface Type field displays "trunk." The neighborIPAddress field displays the IP address of the subtend interface on the parent DSLAM.

Step 6 From the list box on the left, click the parent chassis (this is the trunk).

Step 7 From the left side of the Map Viewer window, within the Subtend hierarchy view, right-click the name of the network interface for the child chassis.

This DSLAM appears as a child of the parent DSLAM subtend interface.

Setting Up a Subtend Configuration Using an NI-2 DSLAM as Parent and NI-1 DSLAMs as Children

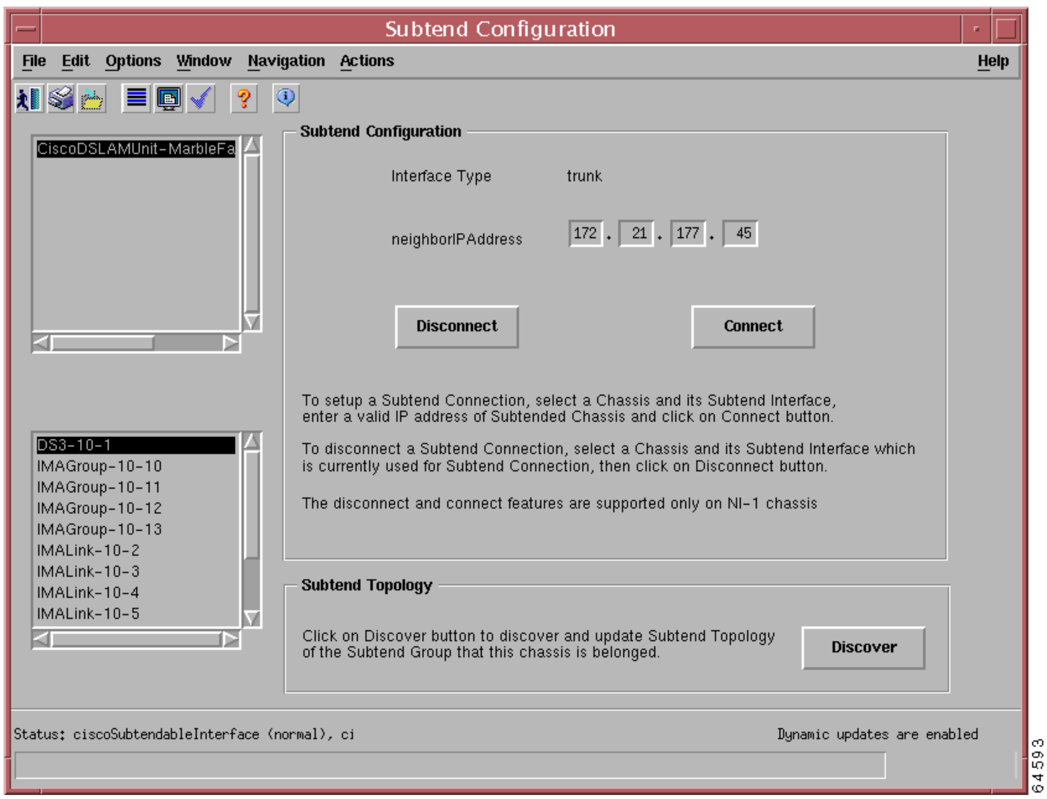
CDM supports a subtend configuration in which an NI-2 DSLAM is the parent of DSLAMs that have NI-1 cards. To set up this type of subtend configuration, complete the following steps. In this type of configuration, the subtend interface of the NI-2 card is connected to the trunk interface of the NI-1 card.

Step 1 From the left side of the Map Viewer window, right-click the **CiscoDSLAMUnit [name of parent chassis]** that you have deployed to access the object menu.

Step 2 Choose **Cisco DSL Subtend Manager > Subtend > Subtend Configuration**.

The Subtend Configuration window opens. (See Figure 5-8.)

Figure 5-8 Subtend Configuration Window



Step 3 From the top list box, highlight the name of the parent DSLAM.

The Interface Type field in the Subtend Configuration area displays "trunk" for the parent chassis interface and displays "subtend" for the child chassis interface.

Step 4 From the lower list box that displays network interfaces, click the interface of this DSLAM chassis.

Step 5 In the Subtend Configuration area neighbor IP Address field, enter the IP address of the child NI-1 DSLAM chassis that you want the parent DSLAM to subtend.

Note When configuring an NI-2 parent DSLAM with NI-2 child DSLAMS, you do not need to use the Subtend Configuration area in this window.

Step 6 Click **Connect**.

CDM connects the child NI-1 DSLAM to the parent NI-2 DSLAM.

Note DSLAMs that are configured with NI-2 cards support the interim link management interface (ILMI) ATM specification. When two NI-2 DSLAMS are connected in a subtend relationship, CDM automatically discovers the neighbor IP address. You do not need to explicitly set up the connection when configuring an NI-2 subtended DSLAM as you do with an NI-1 subtended system. One consequence of ILMI support is that you are unable to disconnect a subtend connection. As long as the DSLAMs are physically connected, the connection is always present.

Disconnecting Two DSLAMs from a Subtend Configuration

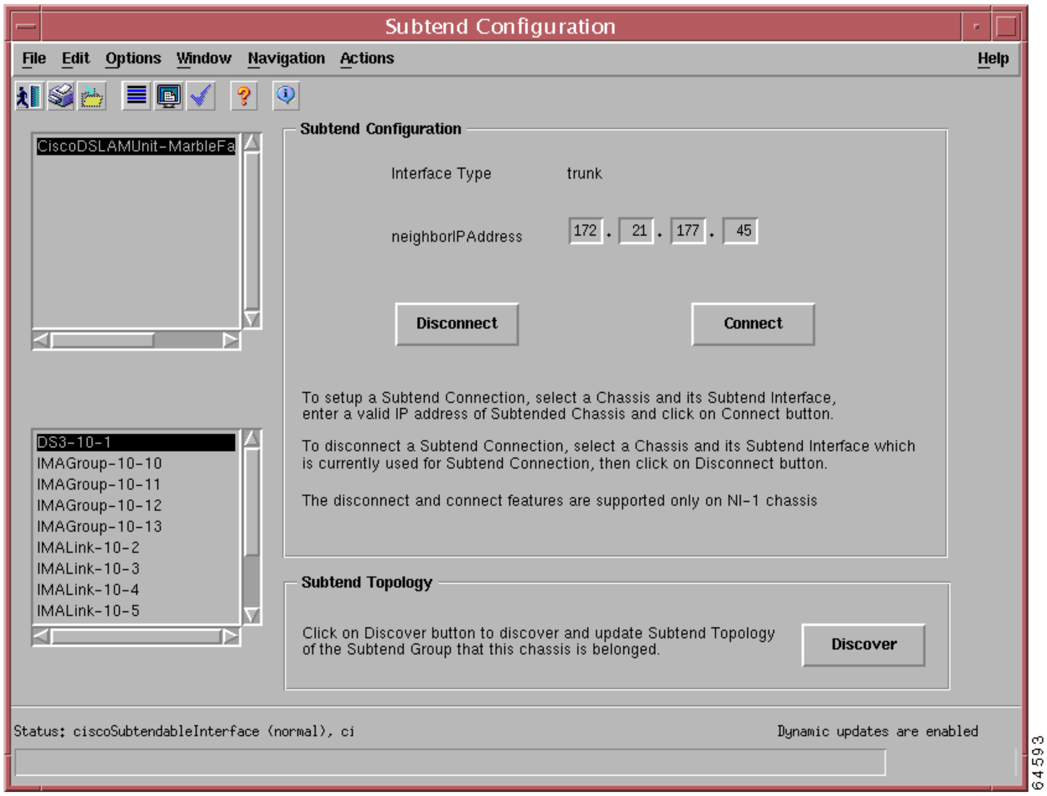
To disconnect an NI-1 child DSLAM from an NI-1 or NI-2 parent DSLAM, complete the following steps:

Step 1 From the left side of the Map Viewer window, right-click the CiscoDSLAMUnit [name of parent chassis] that you have deployed to access the object menu.

Step 2 Choose **Cisco DSL Subtend Manager > Subtend > Subtend Configuration**.

The Subtend Configuration window opens. (See Figure 5-9.)

Figure 5-9 Subtend Configuration Window



Step 3 From the top list box, highlight the name of the parent chassis from which you want to disconnect a child chassis.

The Interface Type field in the Subtend Configuration area displays "trunk" for the parent chassis interface and displays "subtend" for the child chassis interface.

Step 4 From the list box of network interfaces on the left, click the interface of the child chassis.

Step 5 In the Subtend Configuration area neighborIPAddress field, enter the IP address of the child NI-1 DSLAM chassis that you want to disconnect.

Step 6 Click **Disconnect**.

CDM disconnects the child NI-1 DSLAM from the parent NI-2 DSLAM.

Note DSLAMs that are configured with NI-2 cards support the interim link management interface (ILMI) ATM specification. When two NI-2 DSLAMS are connected in a subtend relationship, CDM automatically discovers the neighbor IP address. You do not need to explicitly set up the connection when configuring an NI-2 subtended DSLAM as you do with an NI-1 subtended system.

One consequence of ILMI support is that you are unable to disconnect a subtend connection. As long as the DSLAMs are physically connected, the connection is always present. When you disconnect an NI-2 parent DSLAM that has NI-2 children DSLAMS, you do not use the Subtend Configuration area in the Subtend Configuration window. You only need to click **Discover** for CDM to discover whether the connection is present or absent.

Setting Up Subtended Subscribers

This section includes the following topics:

To set up subscribers in a subtend Cisco DSLAM, you create settings for the child DSLAM subscribers in the same manner as you would any subscribers, by creating and applying profiles. The parent and child chassis and line cards should be present on your system. The parent chassis displays on the left side of the Map Viewer window.

Setting Subscriber PVCs on a Subtend System

Complete the following steps to set PVCs for subscribers on a subtend system. See the "Guidelines for Configuring ATM Virtual Channels" section on page 4-12 for more information on setting PVCs.

Step 1 Right-click the chassis on which you are going to set subtend subscribers and choose **Cisco DSL Manager > Chassis > Administration > IOS Settings** from the object menu.

Step 2 Click the IOS/Command Line Security tab and verify that both the IOS login and exec passwords are set, then close this window.

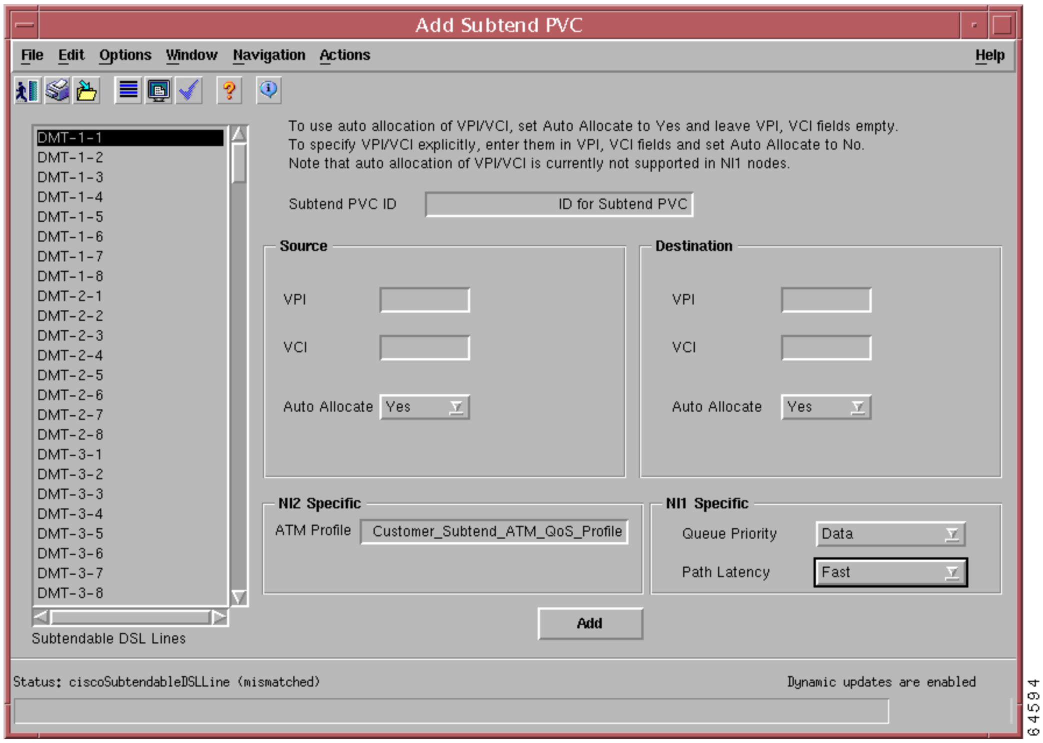
Step 3 From the left side of the Map Viewer window, under the Subtend view, click on the chassis object for which you want to set a subtend subscriber PVC.

Step 4 Right-click this interface name, for example DMT-4-1, to access the object menu.

Step 5 Choose **Cisco DSL Manager > Subtend > Add Subtend PVC**.

The Add Subtend PVC window opens. (See Figure 5-10).

Figure 5-10 Add Subtend PVC Window



Step 6 If you click the chassis to open this window, the names of many line cards display in the list box on the left. In that case, highlight the line card for which you want to create a subtend PVC.

> **Note** For an NI-1 node, the DSL interface should have a subscriber already assigned to it before you can add the subtend PVC.

Step 7 Enter a unique ID in the Subscriber Subtend PVC ID field.

> **Note** See the "Guidelines for Configuring a Subtend System" section on page 5-3 for more information on setting PVCs.

Step 8 Enter appropriate settings in the Source area as follows:

a. In the VPI and VCI fields, enter the values to specify ingress for the subtend network.

b. Alternatively, you can use the down arrow in the Auto Allocate field to select **Yes**.

> **Note** Setting Auto Allocate to Yes is valid only for NI-2 subtend DSLAMS and allows CDM to automatically allocate this pair of values for the subtend network ingress.

Step 9 Enter appropriate settings for the Destination VPIs and VCIs, as follows:

a. In the VPI and VCI fields, enter the values to specify egress for the subtend network.

b. Alternatively, you can use the down arrow in the Auto Allocate field to select **Yes**.

> **Note** Setting Auto Allocate to Yes is only valid for NI-2 subtend DSLAMS, and allows CDM to automatically allocate this pair of values for the subtend network egress.

Step 10 For NI-2 subtend DSLAMs, in the NI2 Specific area ATM Profile field, enter the QoS profile that you want CDM to use for the NI-2 PVC.

Use the tooltips for guidance.

> **Note** If you fail to enter a QoS profile in this field, CDM uses the default profile.

Step 11 For NI-1 subtend DSLAMs, set the following values in the NI1 Specific area of the Add Subtend PVC window (see Figure 5-10):

> **Note** You must set these values for an NI-1 subtend chassis; CDM does not assign default values to these parameters.

a. Use the down arrow in the Queue Priority field to select one of the following:

- Voice
- Voice Signalling
- Data, which is the recommended setting

b. Use the down arrow in the Path Latency field to select **Fast** or **Interleaved**.

Step 12 Click **Add**.

An Action Report window opens to inform you whether this procedure is successful. When CDM has successfully added the PVC, the left side of the Map Viewer window hierarchy view displays the Subtend PVC view. Below this, CDM displays the following information for that specific PVC:

CiscoSubtendPVC_<count of the node in the subtend path from the leaf node>_<Subtend PVC ID>

The leaf node is the lowest level DSLAM in the subtend network, and the root node (root of the subtend network) is the highest level DSLAM in the subtend network. You set the Subtend PVC ID in the Create Subtend PVC window. For example, create a subtend PVC with ID of Bubba on 172.21.177.15 in the following subtend network:

172.21.177.35 (root node) CiscoSubtendPVC_3_Bubba

172.21.177.45 CiscoSubtendPVC_2_Bubba

172.21.177.15 (leaf node) CiscoSubtendPVC_1_Bubba

For NI-2 node PVC objects, you can also see this hierarchy view below the Component Managed View.

Note The NI-1 controller does not add Cisco EMF objects for the PVCs that CDM creates for a particular parent DSLAM. You must verify that individual PVC components are indeed in the node by using a MIB browser or the command line interface (CLI).

The PVC connections that you add display in the map view hierarchy below the interface name. For example:

DMT-1-4
  CiscoSubtendPVC_1_(2)
    CiscoSubtendPVC_1_HighVCL
    CiscoSubtendPVC_1_LowVCL

The High VCL refers to the network side, and the Low VCL refers to the subscriber side.

Deleting Subtend PVCs

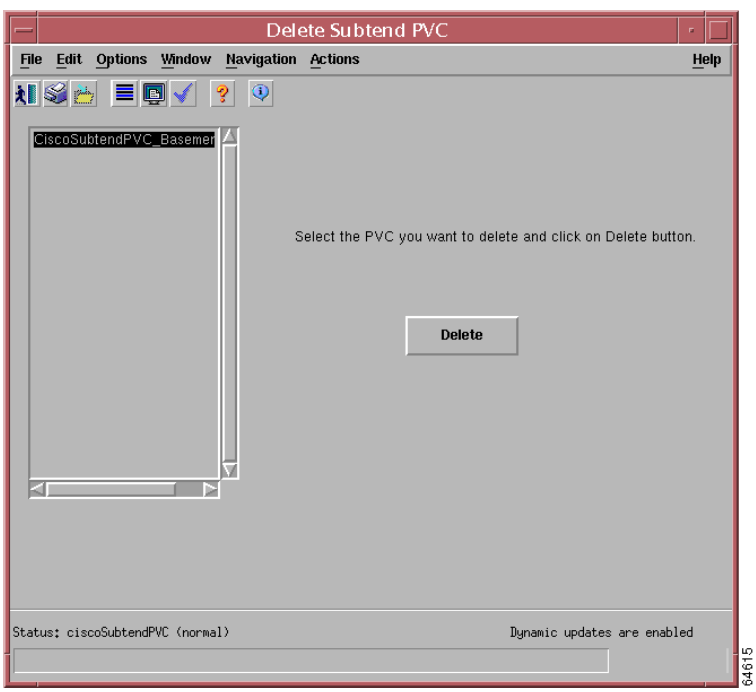
To delete a subtend PVC, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Subtend PVC view, right-click the subtend PVC chassis from which you want to delete a subtended PVC.

Step 2 Choose **Cisco DSL Manager > Delete Subtend PVC** from the object menu.

The Delete Subtend PVC window opens. (See Figure 5-11.)

Figure 5-11 Delete Subtend PVC Window



Step 3 In the list box on the left, click the subtend PVC that you want to delete.

Step 4 Click **Delete**.

An Action Report window opens and displays the details of the deletion process. To verify that CDM has deleted the PVCs, check the Subtend PVC hierarchy view on the left side of the Map Viewer window. All the children from the Subtend PVC that you deleted should no longer display. Any NI-2 PVC objects also should no longer display from the Component Managed view. Verify that CDM has deleted all Subtend PVCs from the node by using an SNMP browser or the CLI.

Maintaining System Performance

This chapter describes how to maintain your Cisco EMF and CDM software system at its peak level of performance.

This chapter includes the following sections:

Viewing and Configuring the System Log File

This section includes the following topics:

The system log file records all system-generated messages for each DSLAM chassis that is configured on the network. The DSLAM logs system messages and sends these messages to the Cisco EMF or CDM software system console. The DSLAM node software, IOS, saves system log messages in an internal buffer that can store up to 1,024 messages.

The system message logging facility allows you to do the following tasks:

- Monitor and troubleshoot your system
- Select the severity levels of the captured information

You can view or print system log information from the SysLog Messages window, which is shown in Figure 6-1. The SysLog Messages window contains a list of network elements from which you select the element whose error and status messages you want to view. Examples of messages that can appear in the SysLog Messages window for a network element include alarm messages or loss of traffic messages.

Configuring the System Log Message Details

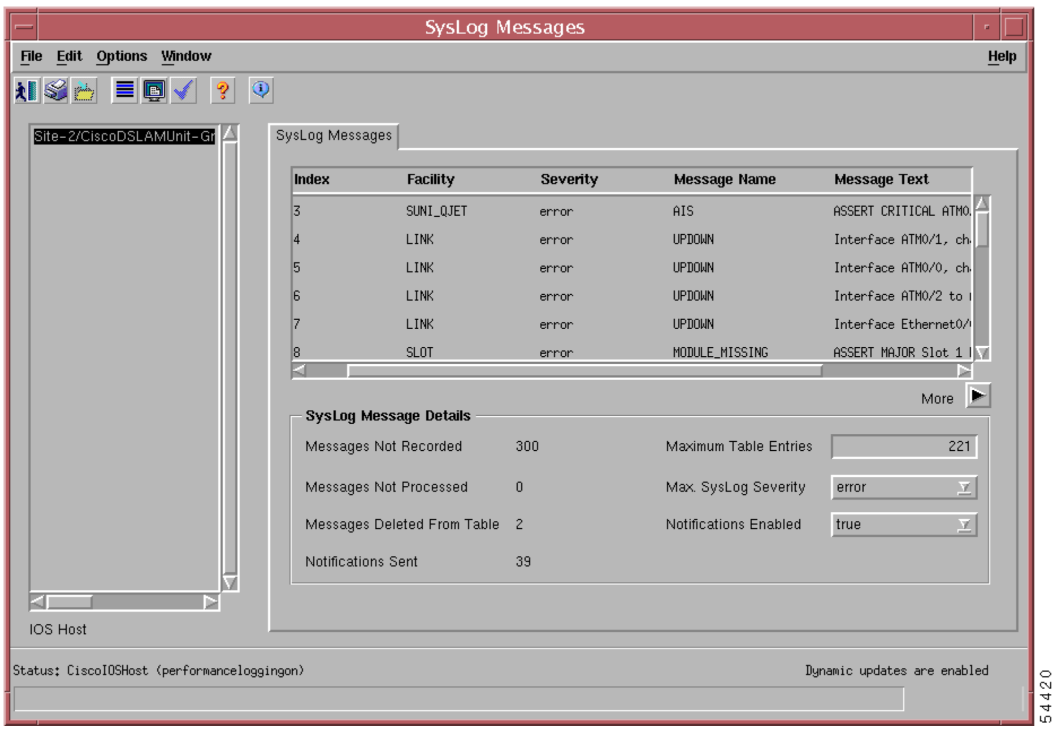
To configure the system log messages details in the SysLog Messages window, complete the following steps:

Step 1 In the Map Viewer window, within the Physical view, right-click the chassis whose system log messages you want to view.

Step 2 Choose **Cisco DSL Manager > Chassis > Tools > Logging > View Error Log**. from the object menu.

The SysLog Messages window opens. (See Figure 6-1.)

Figure 6-1 SysLog Messages Window



The SysLog Messages area at the top of the SysLog Messages window includes a number of columns; use the scroll bar to view all of the columns. CDM displays the relevant information about each syslog message in these columns. Table 6-1 describes the fields in this window.

Step 3 From the list box on the left side of the window, select the chassis whose system log you want to view.

Step 4 Configure the parameters on the right side of the SysLog Messages Details area:

a. In the Maximum Table Entries field, enter the number of events you want to view at one time; this value sets the upper limit on the number of entries the table can contain.

b. In the Max. SysLog Severity field, use the down arrow to select the severity level of events you want to view; the agent ignores any message for events whose severity is lower than this level.

See Table 6-2 for definitions of the severity levels.

c. In the Notifications Enabled field, use the down arrow to select your preference for alarm notification, as follows:

- Select **true** if you want to be notified of alarms (alarms display in the list of events in the SysLog Messages area).
- Select **false** if you do not want to be notified of alarms.

Step 5 Click **Save** to save your settings.

The list of events appear in the SysLog Messages area as shown in Figure 6-1.

SysLog Messages Window Field Descriptions and Severity Level Descriptions

Table 6-1 defines the fields in the SysLog Messages window.

Table 6-1 Syslog Messages Window Field Descriptions

Field	Description
SysLog Messages	
Index	Displays the message index number.
Facility	Displays the name of the facility that generated the message.
Severity	Displays the level of severity of the error (see Table 6-2).
Message Name	Displays the unique message type.
Message Text	Displays the text of the message.
Time Stamp	Identifies the time the message was generated (SysUpTime).
SysLog Message Details	
Messages Not Recorded	Displays the number of messages that have not been recorded.
Messages Not Processed	Displays the number of messages that have not been processed.
Messages Deleted From Table	Displays the number of messages that have been deleted from the table.
Notifications Sent	Displays the number of notifications that have been sent.
Maximum Table Entries	Enter the upper limit on the number of entries that the table can contain.
Max. SysLog Severity	Use the down error to select the level of events you want the agent to display (see Table 6-2 for a list of severity levels). The agent will ignore any message for events whose severity is lower than this level.
Notifications Enabled	Use the down arrow to select true to enable notifications, or false to not enable notifications.

In the SysLog Messages window Max SysLog Severity field, you can select a severity range for the events that you want to view. Table 6-2 describes the severity levels.

Table 6-2 SysLog Messages Window Severity Level Definitions

Level	Definition
Emergency	The system is unusable.
Alert	Immediate action is required.
Critical	Prompt action is required.
Error	Necessary action is required.
Warning	A minor condition has occurred.
Notice	A normal but significant condition has occurred.
Info	Informational messages are captured.
Debug	Debugging messages are captured.

The Emergency level is the most severe type of message that the system generates (the level that you set in the Max SysLog Severity field); the Debug severity level is the least severe type of message. For example, if you select a maximum severity level of

- Emergency—The window displays only the error and status messages with an Emergency severity level.
- Warning—The window displays all messages from the Warning severity level up to the Emergency severity level (within the date range that you selected), and ignores all messages below the Warning severity level.
- Debug—The window displays all messages for all severity levels.

Note After you configure or change the parameters, the system does not dynamically update the list of events in the SysLog Messages area. Only the syslog messages that the system generates since you configured the parameters display in the SysLog Messages area.

Note CDM logs user-initiated events in the Command History window (see the following section, Viewing and Configuring the Command Log Window, for more information.)

Viewing and Configuring the Command Log Window

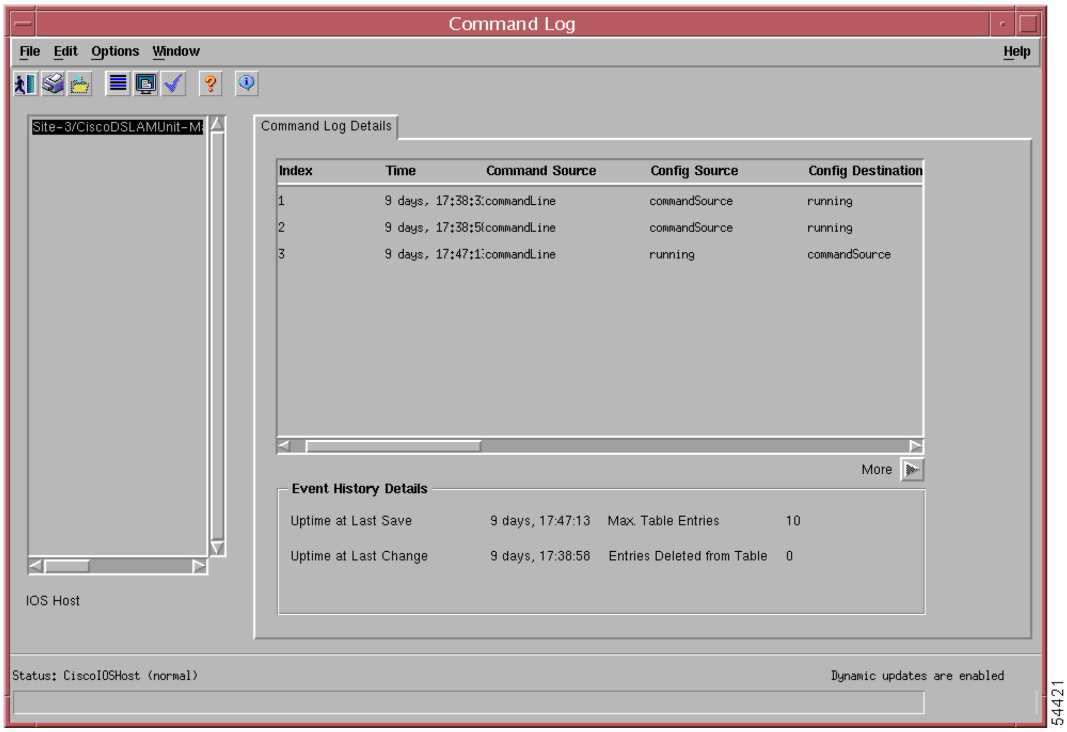
The Command Log window reflects the data that is in the Command History file, which is a system-generated file. Each time a user makes a configuration change to a network element, the system creates an entry in the Command History file.

From the Command Log window, which is shown in Figure 6-2, you can view the details of each configuration entry including the following event information:

- Event Index
- Time the event occurred
- Name of the logged-in user

- Change that was performed on an object
- Internet address of the requested system or requester

Figure 6-2 Command Log Window



To open and configure the Command Log window opens. (See Figure 6-2.) Complete the following steps to open the Command Log window:

Step 1 From the Map Viewer window, within the Physical view, right-click a chassis object to access the object menu.

Step 2 Choose **Cisco DSL Manager > Chassis** > **Tools > Logging** > **View Command History**.

The Command Log window opens. (See Figure 6-2.)

Step 3 From the list box on the left side of the window, select the chassis whose command history events you want to view.

Step 4 Use the scroll bar at the bottom of the Command Log Details area to view all of the columns.

Step 5 Click the **Refresh** button in the toolbar, then click the arrow next to More to add entries to the table.

Note After you configure or change the parameters, CDM does not dynamically update the list of events in the Command Log Details area. Only the messages that CDM generates since you configured the parameters display in the Command Log Details area.

Command Log Window Field Descriptions

Table 6-3 describes the fields that display events in the Command Log Details area.

Table 6-3 Command Log Field Descriptions

Column Name	Description
Command Log Details	
Index	Displays the index number of the event.
Time	Displays the value of sysUpTime when the event occurred. In the example in Figure 6-2, the configuration had been running for 9 days, 17 hours, 38 minutes, and 3 seconds.
Command Source	Displays the source of the command that instigated the event, for example the command line or snmp.
Config Source	Displays the configuration data source for the event, for example, running configuration or command source.
Config Destination	Displays the configuration data destination for the event, for example, running configuration or startup configuration.
Terminal Type	Displays the terminal type from which the event was logged, either virtual or not applicable.
Terminal Number	Displays the number of the terminal from which the event was logged.
Terminal User	Displays the name of the logged in user of the terminal from which the event was logged.
Terminal Location	Displays the hard-wired location of the terminal or remote host from which the event was logged.
Command Source Address	Displays the Internet address of the connected system or system from which the request originated.
Virtual Host Name	Displays the virtual host name of the connected system.
Server Address	Displays the Internet address of the storage file server.
File	Displays the configuration file name of the storage file server.
RCP User	Displays the name of the remote user.
Command Log Details	
Uptime at Last Save	Displays the value of sysUpTime when the running configuration was last saved.
Uptime at Last Change	Displays the value of sysUpTime when the running configuration was last changed.
Max. Table Entries	Displays the maximum number of entries that can be held in the table.
Entries Deleted from Table	Displays the number of times that a new event caused the oldest event at that time to be deleted in order to make room for the new event.

Setting Telnet Passwords

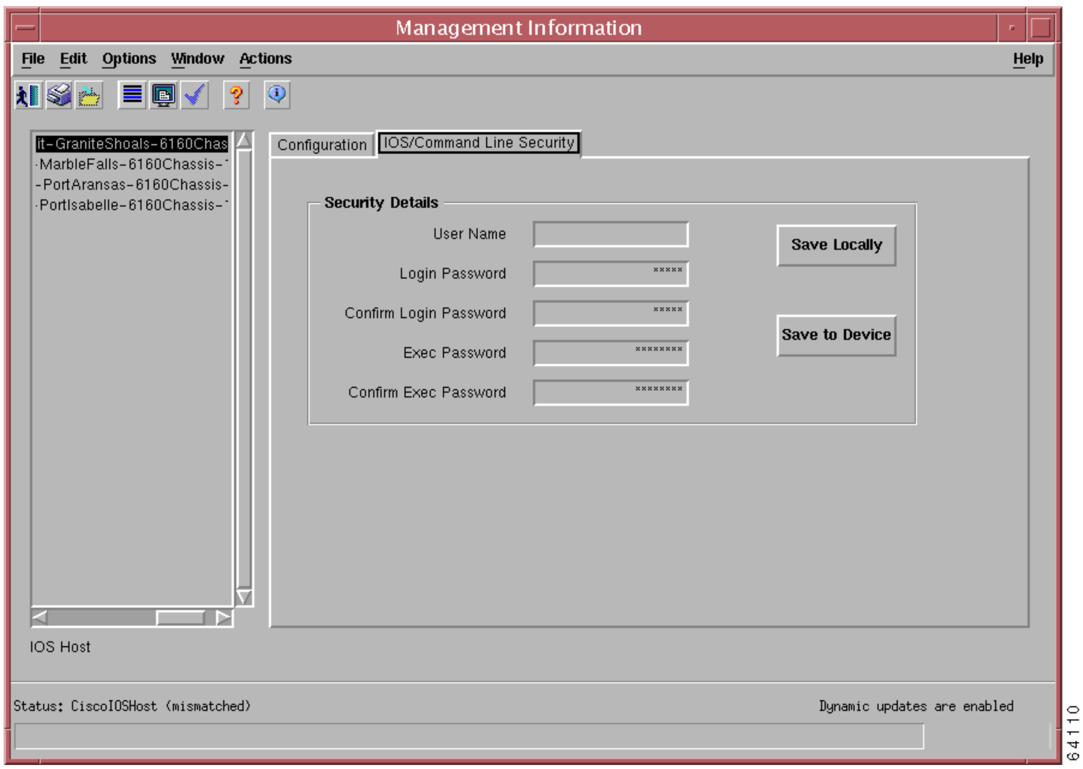
Setting Telnet passwords is the same process as setting IOS CLI security passwords. You need to make sure you have configured your Telnet passwords in CDM. Setting the Telnet passwords allows you to open a Telnet window from the CDM GUI and communicate with the DSLAM using IOS commands. If you have not already set the security password for a DSLAM, complete the following steps to check Telnet passwords:

Step 1 In the Map Viewer window, within the Physical view, right-click the chassis object for which you want to set the Telnet password.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > IOS Settings** from the object menu.

The Management Information window opens. (See Figure 6-3.)

Figure 6-3 Management Information Window—IOS/Command Line Security Tab



In the IOS/Command Line Security tab, you are informing CDM what the IOS passwords are so that CDM can run IOS scripts.

Step 3 Click the **IOS/Command Line Security** tab opens. (See Figure 6-3.)

Step 4 Enter your login password in the Login Password field.

Step 5 Enter the password again in the Confirm Login Password field.

Step 6 Enter the executive password in the Exec Password field.

Step 7 Enter the executive password again in the Confirm Exec Password field.

The procedure here is parallel to that in IOS, when you use the **enable** command and then enter the exec password to go into the executive mode.

Step 8 Click **Save Locally** to save your passwords locally to CDM.

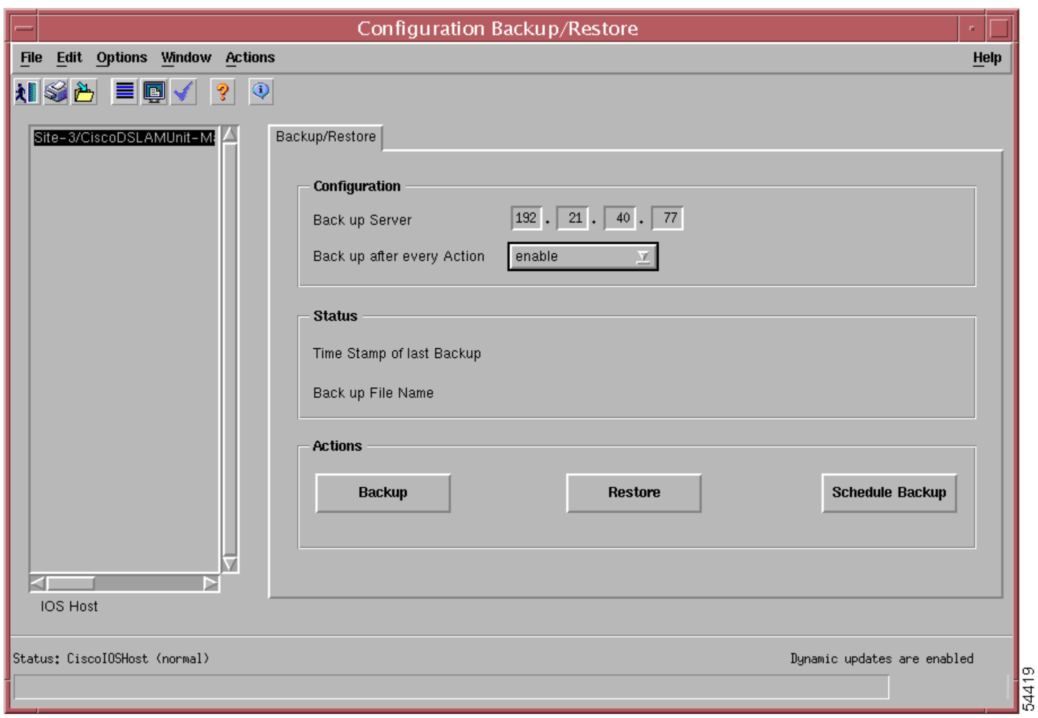
Step 9 Click the **Save** icon in the toolbar.

Backing Up and Restoring Configuration Information

To back up configuration data from your DSLAM, you can upload the currently running Cisco DSLAM configuration and save it as a file to any TFTP server. You can download this file later from the TFTP server to a specified Cisco DSLAM.

Cisco recommends that you perform backups on a regular basis to recover configuration information in the unlikely event of a hardware failure. For example, if an NI-2 card fails, you can install a new NI-2 card in the chassis, click the Restore button in the Configuration Backup/Restore window, and the system restores the configuration data. The Configuration Backup/Restore window is shown in Figure 6-4.

Figure 6-4 Configuration Backup/Restore Window



It is important that you back up configuration data on a regular basis because all configuration changes made between the last backup and the time of the failure will be lost.

Note The backup/restore feature is not intended for use as a configurable tool. The system uses the same file each time you back up the configuration data.

Backup/Restore is configured on a per chassis basis. When you click the Backup button, the running configurations of the DSLAM is copied onto the TFTP server. When you click the Restore button, the system restores the most recently saved running configuration to a Cisco DSLAM.

To open the Configuration/Backup Restore window and perform a backup and restore of your configuration data, follow these steps:

Step 1 From the Map Viewer window, right-click the shelf or chassis whose configuration data you want to backup.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > Configuration Backup/Restore** from the object menu.

The Configuration Backup/Restore window opens. (See Figure 6-4.)

Step 3 From the list on the left side of the window, select the chassis, or multiple cards, for which you want to back up or restore configuration data.

Step 4 Configure the parameters in the Configuration area as follows:

a. In the Back Up Server field, enter the TFTP IP address of the backup server.

b. Leave the Back Up After Every Action field blank, or use the down arrow to select **Disable**.

The Time Stamp of Last Backup field is *Display only*. This field displays the time that the system last backed up the configuration data.

The Back Up File Name is *Display only*. This field displays the name of the last backed up file. The file name does not change. The file name is based on the chassis IOS Host name and IP address, and is used for each backup session.

Note At this time, you must save the information that you entered before you click **Backup**, **Restore**, or **Schedule Backup** in the following steps. If you do not save the information that you entered, CDM uses the information that was previously entered and saved in this file instead of the information that you just entered.

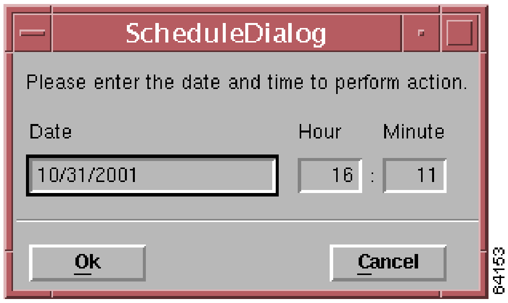
Step 5 Choose **File > Save** from the menu bar or click the Save icon in the toolbar.

Step 6 Perform one of the following actions depending on your purpose:

- Click **Backup** to immediately start backing up the currently running configuration of a Cisco DSLAM.
- Click **Restore** to immediately start restoring the currently running configuration to a Cisco DSLAM.
- Click **Schedule Backup** to schedule a later date and time for the backup to take place.

If you click **Schedule Backup**, the Schedule Dialog dialog box opens. (See Figure 6-5.)

Figure 6-5 Configuration Backup/Restore—Schedule Dialog Window



Step 7 Enter the date (mm/dd/yyyy) and time (24-hour format, for example, 4:00 p.m. is 16:00) that you want the system to perform the backup.

Step 8 Click **OK** to save the new date and time.

Downloading a Cisco IOS Software Image

When Cisco releases a new version of Cisco IOS, you can download the new version of the software onto a DSLAM chassis. From the IOS Image Download window, you define the parameters to maintain the most current Cisco IOS software on the DSLAM chassis in your network.

Note Before you download a new Cisco IOS software image you must configure the SNMP information. To verify whether the SNMP information is configured, open the SNMP Management window (see the "Enabling SNMP Trap Generation" section on page 2-47).

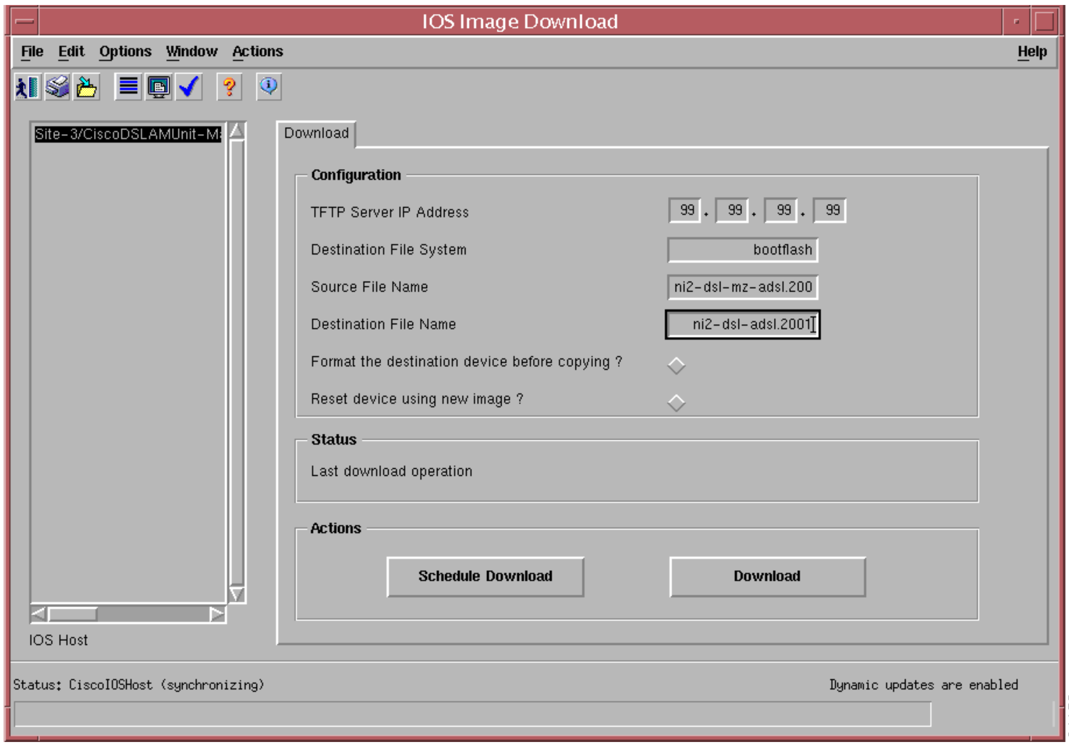
To download a new Cisco IOS software image, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the chassis for which you want to download a new IOS image.

Step 2 Choose **Cisco DSL Manager > Chassis > Administration > IOS Image Download** from the object menu.

The IOS Image Download window opens. (See Figure 6-6.)

Figure 6-6 IOS Image Download Window



The chassis that you selected is highlighted in the list box on the left side of the window.

Step 3 Configure the Cisco IOS image download values as follows:

a. In the TFTP Server IP Address field, enter the IP address of the TFTP server that contains the Cisco IOS image software you want to download.

b. In the Destination File System field, enter the destination file system name; valid values are bootflash or flash.

c. In the Source File Name field, enter the name of the source file; you can specify the Cisco IOS image download source file name.

d. In the Destination File Name field, enter the path and file name of the destination file.

You can specify the name for the file as it is stored in the file system of CDM.

e. In the Format the destination device before copying? field, click the diamond if you want to erase the software on the chassis before the new software is downloaded.

If you do not click this option to format the destination device, the file does not get overwritten and you might run out of space; it is best to format the destination device.

f. In the Reset device using new image? field, click the diamond if you want to reset the chassis to start using the new software.

The Last download operation field is *Display only*. This fields displays the date and time of the last download.

Note At this time, you must save the information that you have entered before you click **Download** or **Schedule Download**. If you do not save the information that you have entered, the software returns an error message when you attempt to download or schedule a download.

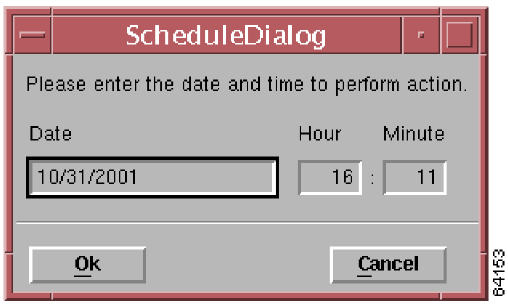
Step 4 Choose **File > Save** from the menu bar or click the Save icon in the toolbar.

Step 5 Click **Schedule Download** to schedule the download to be performed at a later time.

Step 6 Click **Download** to perform the download immediately.

When you click **Schedule Download**, the Schedule Dialog dialog box opens. (See Figure 6-7.)

Figure 6-7 Cisco IOS Download—Schedule Dialog



Step 7 Enter the date (mm/dd/yyyy) and time (24-hour format, for example, 4:00 p.m. is 16:00) you want the system to perform the download, and then click **OK**.

Saving the Running Configuration to Memory

You can save the configuration by issuing a **write mem** command from the Chassis Configuration window. You do this by choosing writeMem from the Actions menu in this window to save the running configuration.

You can also save the running configuration by following these steps:

Step 1 Click the chassis whose running configuration you want to save.

Step 2 Choose **Cisco DSL Manager > Technology Commands > Save Running Config** from the object menu.

A Telnet window opens and displays the results of saving the configuration. You must have user name and password set to the DSLAM.

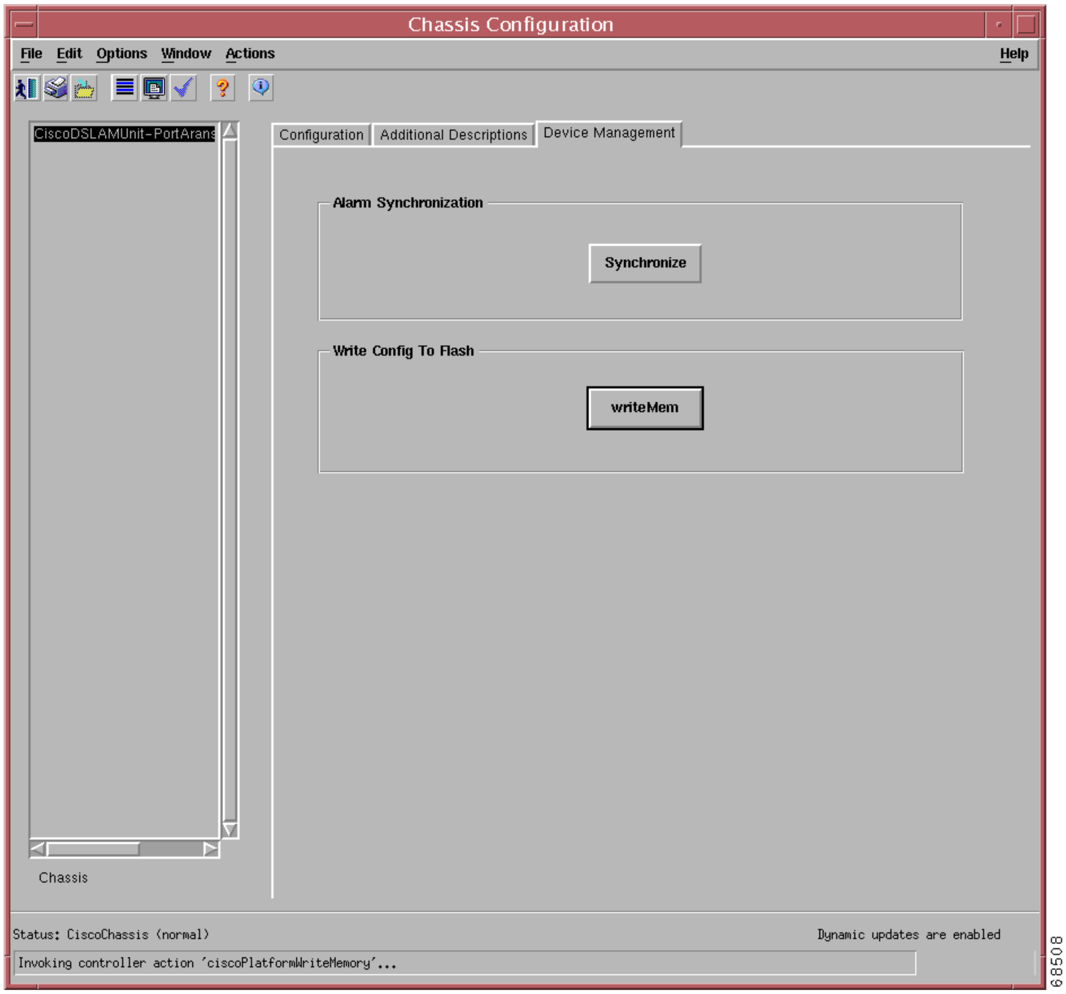
Step 3 Click **Close** to close the telnet window.

Another way to save the configuration to flash is as follows:

Step 1 Open the Chassis Configuration window by right-clicking a chassis (DSLAM) object and choosing **Cisco DSL Manager > Chassis > Configuration** from the object menu.

The Chassis Configuration window opens. (See Figure 6-8.)

Figure 6-8 Chassis Configuration Window—Device Management Tab



Step 2 In the Write Config To Flash area, click **writeMem**.

Synchronizing Alarms

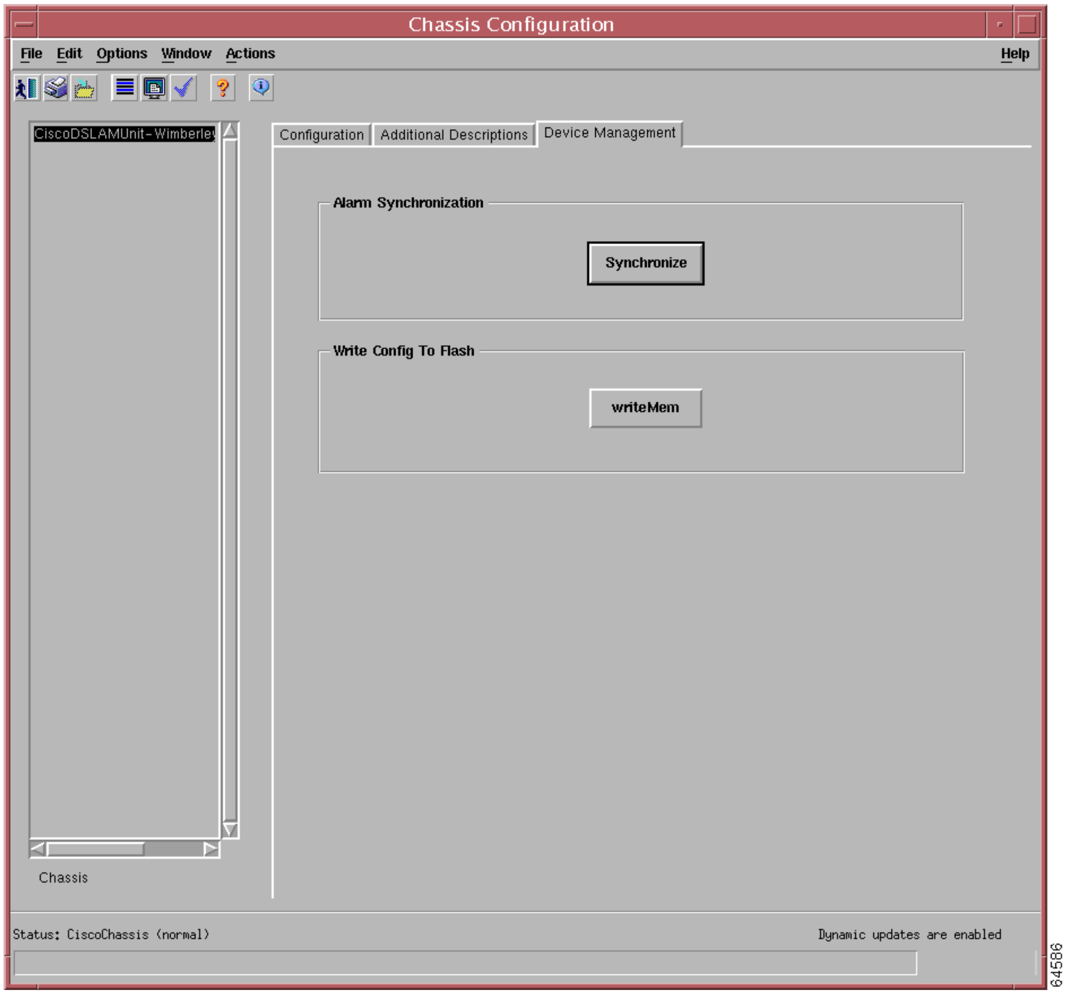
You can synchronize all alarms for a DSLAM by using the Alarm Synchronization feature. Doing this initiates a search for all traps on a DSLAM, displays them in the Event Browser, and populates the Map Viewer window hierarchy views to reflect all discovered alarms.

Complete these steps to synchronize all alarms:

Step 1 Open the Chassis Configuration window by right-clicking a chassis (DSLAM) object and choosing **Cisco DSL Manager > Chassis > Configuration** from the object menu.

The Chassis Configuration window opens. (See Figure 6-9.)

Figure 6-9 Chassis Configuration Window—Device Management Tab



Step 2 In the Alarm Synchronization area, click **Synchronize**.

For more information about populating alarms in the map hierarchy view, see the "Using the Map Hierarchy Views" section on page 1-33. For more information about viewing alarms in the Event Browser and alarm descriptions, see Appendix A, "Viewing Alarms and Events."

Viewing System and Object Status

This chapter describes the windows in CDM that you can open to observe system and network object status.

This chapter describes how to view status information about the following objects:

Note SONET information is equivalent to OC-3 interface information.

Viewing Chassis Fault Management Status

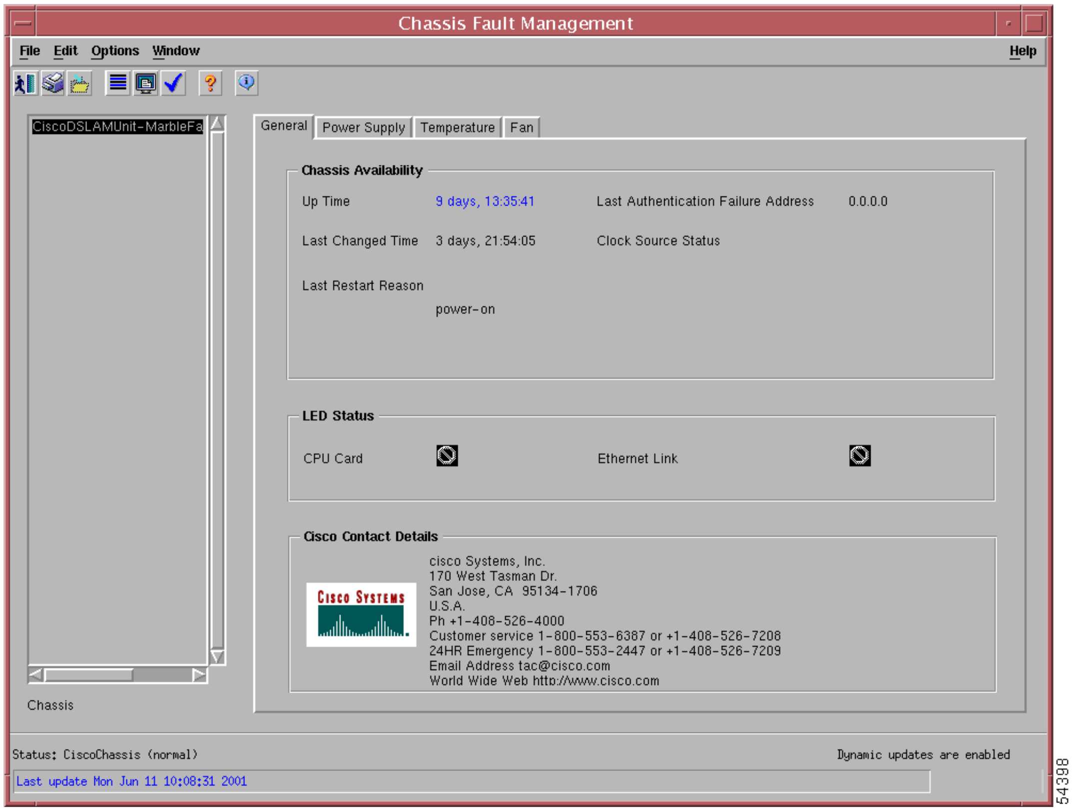
You can view chassis availability details in the Chassis Fault Management window. Complete the following steps to open the Chassis Fault Management window:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click a chassis whose fault management status you want to view.

Step 2 Choose **Cisco DSL Manager > Chassis > Fault Management** from the object menu.

The Chassis Fault Management window opens. (See Figure 7-1.)

Figure 7-1 Chassis Fault Management Window—General Tab



The chassis that you selected is highlighted in the list box on the left side of the Chassis Fault Management window.

The Chassis Fault Management window has four tabs:

- General
- Power Supply
- Temperature
- Fan

Note Only the General tab applies to CDM for Cisco DSLAMs for this release; the other three tabs are not used.

The General tab contains three areas—Chassis Availability, LED Status (which is not applicable for this release of CDM), and Cisco Contact Details. The fields in the General tab are described in Table 7-1.

Table 7-1 Chassis Fault Management Window—General Tab Field Descriptions

Field	Description
Chassis Availability	
Up Time	Displays the up time since the last reset
Last Changed Time	Displays the time when the chassis was last modified.
Last Restart Reason	Displays the reason for the last restart.
Last Authentication Failure Address	Displays the last authorization failure IP address for the selected chassis.
Clock Source Status	Not used.
LED Status	
CPU Card	Not used.
Ethernet Line	Not used.
Cisco Contact Details	Displays contact information for Cisco.

Viewing Generic Interface Status

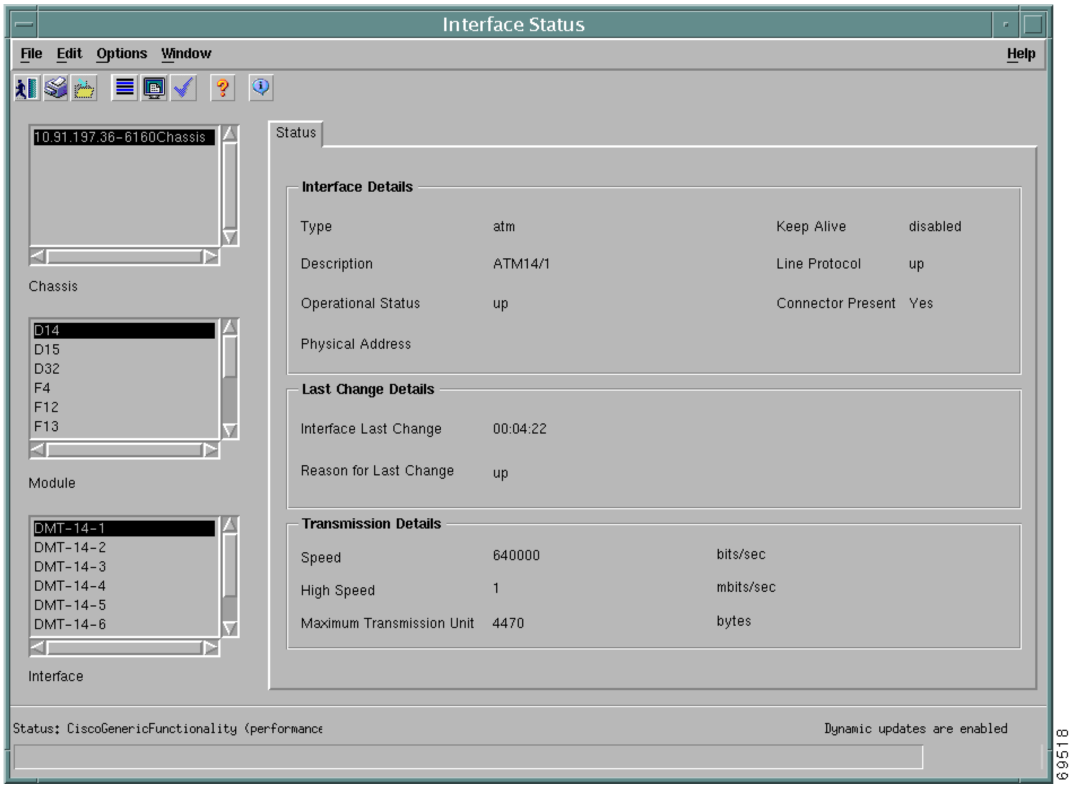
The generic Interface Status window displays status information for any selected interface. To view interface status information, follow these steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the line card whose interface status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > XDSL > Generic** from the object menu.

The Interface Status window opens. (See Figure 7-2.)

Figure 7-2 Interface Status Window



The chassis, card, and interface that you selected is highlighted in the list boxes on the left side of the Interface Status window.

The corresponding details for the selected card display on the right. The Status tab contains three areas:

- Interface Details
- Last Change Details
- Transmission Details

The fields in these three areas are described in Table 7-2.

Table 7-2 Interface Detail Area Field Descriptions

Field	Description
Interface Details	
Type	Displays the interface type.
Description	Displays a text string description of the interface.
Operational Status	Displays the current operational status of the interface.
Physical Address	Not used.
Keep Alive	Indicates whether keepalives are enabled on this interface.

Table 7-2 Interface Detail Area Field Descriptions (continued)

Field	Description
Line Protocol	Indicates whether the line interface protocol is operating.
Connector Present	Specifies whether the interface has a physical connector. True indicates that a physical connector is present; False indicates that a physical connector is not present.
Last Change Details	
Interface Last Change	Displays the value of the system up time at the time the interface entered its current operational state.
Reason for Last Change	Specifies the reason for the last status change of the interface.
Transmission Details	
Speed	Displays an estimate of the current bandwidth for the interface in bits per second.
High Speed	Displays an estimate of the current bandwidth for the interface in units of 1,000,000 bits per second.
Maximum Transmission Unit	Identifies the size of the largest packet that can be sent or received on the interface, specified in bytes.

Viewing T1/E1 Interface Status

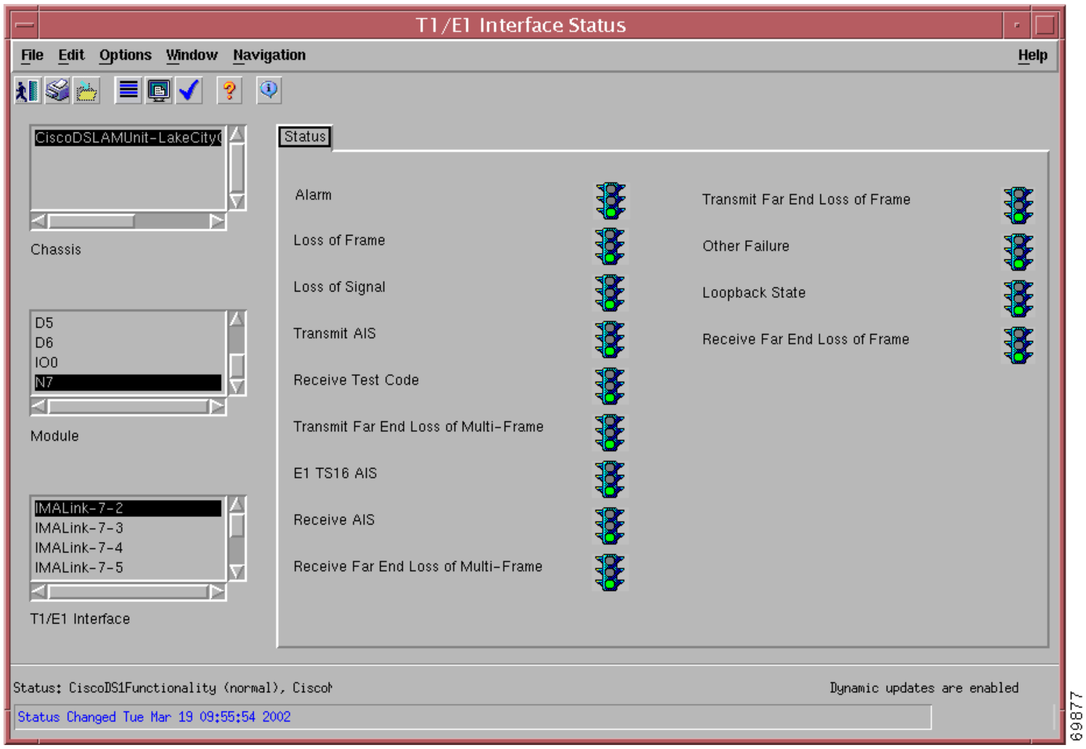
The T1/E1 Interface Status window displays status information for a selected T1 or E1 interface. To view the T1/E1 Interface Status window, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the NI-2 line card whose T1 or E1 status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > T1/E1** from the object menu.

The T1/E1 Interface Status window opens. The T1/E1 Interface Status window has one tab, the Status tab. (See Figure 7-3.)

Figure 7-3 T1/E1 Interface Status Window



The chassis, card, and T1/E1 interface that you selected is highlighted in the list boxes on the left side of the window. If not, click the appropriate interface from the list box on the left to highlight it.

The status information for the selected T1 or E1 interface displays on the right.

Note Black boxes with slashed circles indicate that CDM was unable to retrieve any values for that field. Red indicates the presence of the condition; green indicates an absence of the condition.

The Status tab displays T1/E1 interface status information. The fields in this window are described in Table 7-3.

Table 7-3 T1/E1 Interface Status Window Field Descriptions

Field	Description
Alarm	Indicates the presence or absence of defects in the line.
Loss of Frame	Indicates the presence or absence of frame loss in the line.
Loss of Signal	Indicates the presence or absence of signal loss in the line.
Transmit AIS	Indicates whether an alarm signal is being transmitted.

Table 7-3 T1/E1 Interface Status Window Field Descriptions (continued)

Field	Description
Receive Test Code	Indicates whether the line is receiving a test pattern.
Transmit Far End Loss of Multi-Frame	Indicates whether loss of multi-frame is being transmitted by the far end.
E1 TS16 AIS	Indicates the presence or absence of E1 or TS16 alarm signal.
Receive AIS	Indicates whether a remote alarm signal is being transmitted.
Receive Far End Loss of Multi-Frame	Indicates the presence or absence of loss of multi-frame in the far end line.
Transmit Far End Loss of Frame	Indicates the presence or absence of loss of multi-frame by the near end line.
Other Failure	Indicates the presence or absence of some other failure in the line.
Loopback State	Indicates whether a received signal is looped back.
Receive Far End Loss of Frame	Indicates the presence or absence of a loss of frame in the far end line.

Viewing DS3/E3 Interface Status

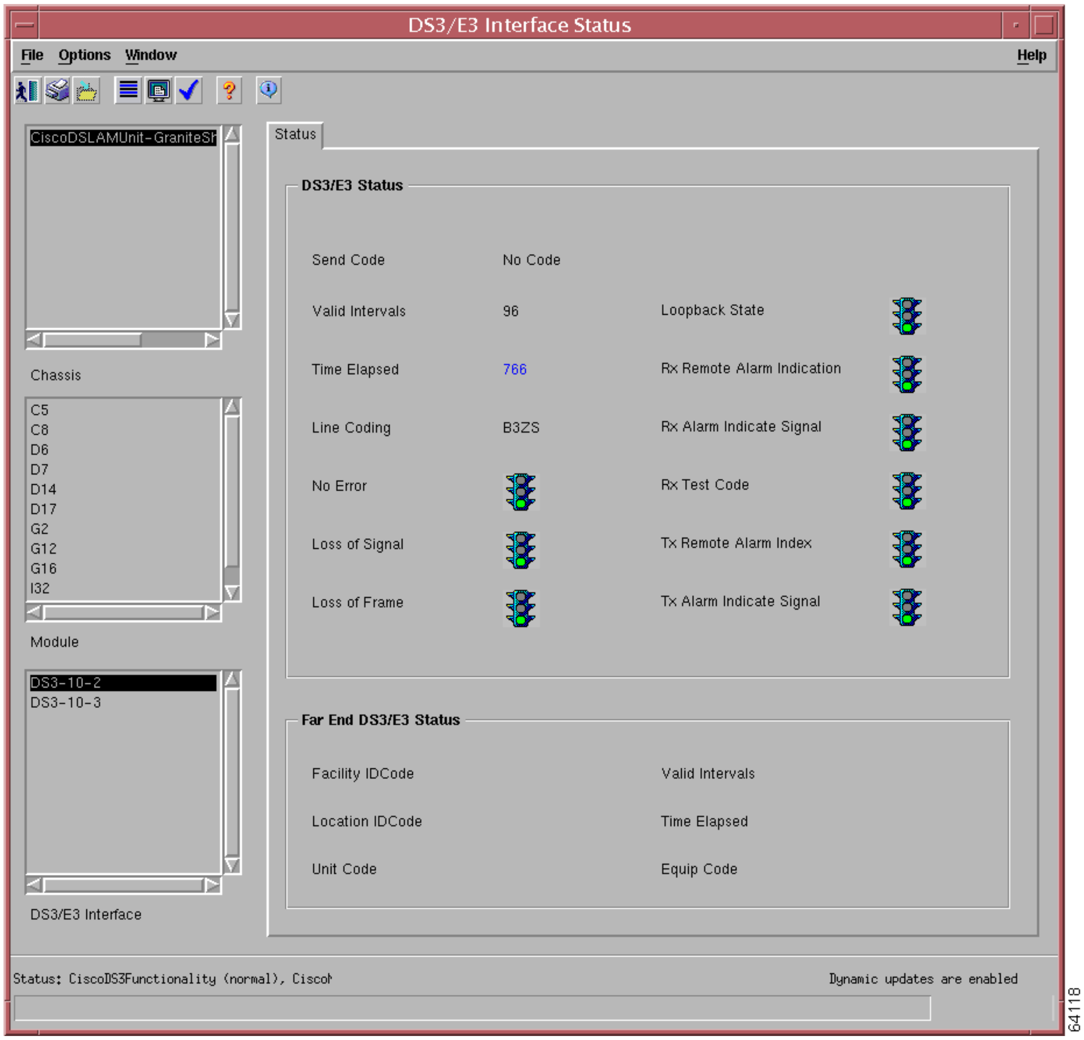
The DS3/E3 Interface Status window displays status information for a selected DS3 or E3 interface. To view the DS3/E3 Interface Status window, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the NI-2 line card whose DS3 or E3 status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > DS3/E3** from the object menu.

The DS/E3 Interface Status window opens. The DS3/E3 Interface Status window has one tab, the Status tab. (See Figure 7-4.)

Figure 7-4 DS3/E3 Interface Status Window



The chassis, card, and DS/E3 interface that you selected is highlighted in the list boxes on the left side of the window. If not, click the appropriate DS3 interface from the list box on the left to highlight it.

The status information for the selected DS3 or E3 interface displays on the right.

Note Black boxes with slashed circles indicate that CDM was unable to retrieve any values for that field. Traffic lights display green if the status is OK; yellow if the status is Warning; and red if the status is Errored.

The Status tab displays DS3/E3 interface status information. The Status tab contains two areas—DS3/E3 Status and Far End DS3/E3 Status. The fields in this window are described in Table 7-4.

Table 7-4 DS3/E3 Interface Status Window Field Descriptions

Field	Description
DS3/E3Status	
Send Code	Indicates the type of code that the device is sending the DS3/E3[1] interface. Send codes are optional for E3 interfaces. Possible values are as follows: • No Code—Sending looped or normal data • Line Code—Sending a request for a line loopback • Payload Code—Sending a request for a payload loopback (for example, all DS1/E1s in a DS3/E3 frame) • Reset Code—Sending a loopback deactivation request • DS1 Loop Code—Requesting to loop back a particular DS1/E1 within a DS3/E3 frame • Test Pattern—Sending a test pattern
Valid Intervals	Displays the number of previous intervals for which valid data is stored.
Time Elapsed	Displays the time elapsed (in seconds) since the beginning of the current error-measurement period. • Transmit Clock Source—Allows you to specify the source of the transmit clock. • Loop Timing—Indicates that the recovered receive clock is used as the transmit clock. You can set this option to: – Free Running—Indicates that a local clock source is used. – Network Derived—Indicates that the recovered receive clock from another interface is used as the transmit clock source.
Line Coding	Displays the type of line coding used in the interface.
No Error	Indicates no alarm is present.
Loss of Signal	Indicates the loss of signal condition.
Loss of Frame	Indicates the loss of frame condition.
Loopback State	Indicates that the interface is looping the received signal.
Rx Remote Alarm Indication	Receiving a remote alarm indication failure signal.
Rx Alarm Indicate Signal	Receiving a remote alarm indication signal.
Rx Test Code	Indicates reception of a test pattern.
Tx Remote Alarm Index	Transmitting a remote alarm index signal.
Tx Alarm Indicate Signal	Transmitting an alarm indication signal.
Far End DS3/E3 Status	
Facility ID Code	Displays the code that identifies a specific far-end DS3 path.
Location ID Code	Displays the far-end location identification code that describes the specific location of the equipment.

Table 7-4 DS3/E3 Interface Status Window Field Descriptions (continued)

Field	Description
Unit Code	Displays the far-end code that identifies the equipment location within a bay.
Valid Intervals	Specifies the number of previous far-end intervals for which valid data was collected.
Time Elapsed	Specifies how much time has elapsed after the current far-end measurement began.
Equip Code	Displays the far-end equipment code that describes the specific piece of equipment.

1. E3 = wide area digital transmission scheme that is used predominantly in Europe and carries data at a rate of 34.368 Mbps.

Viewing ATM Interface Status

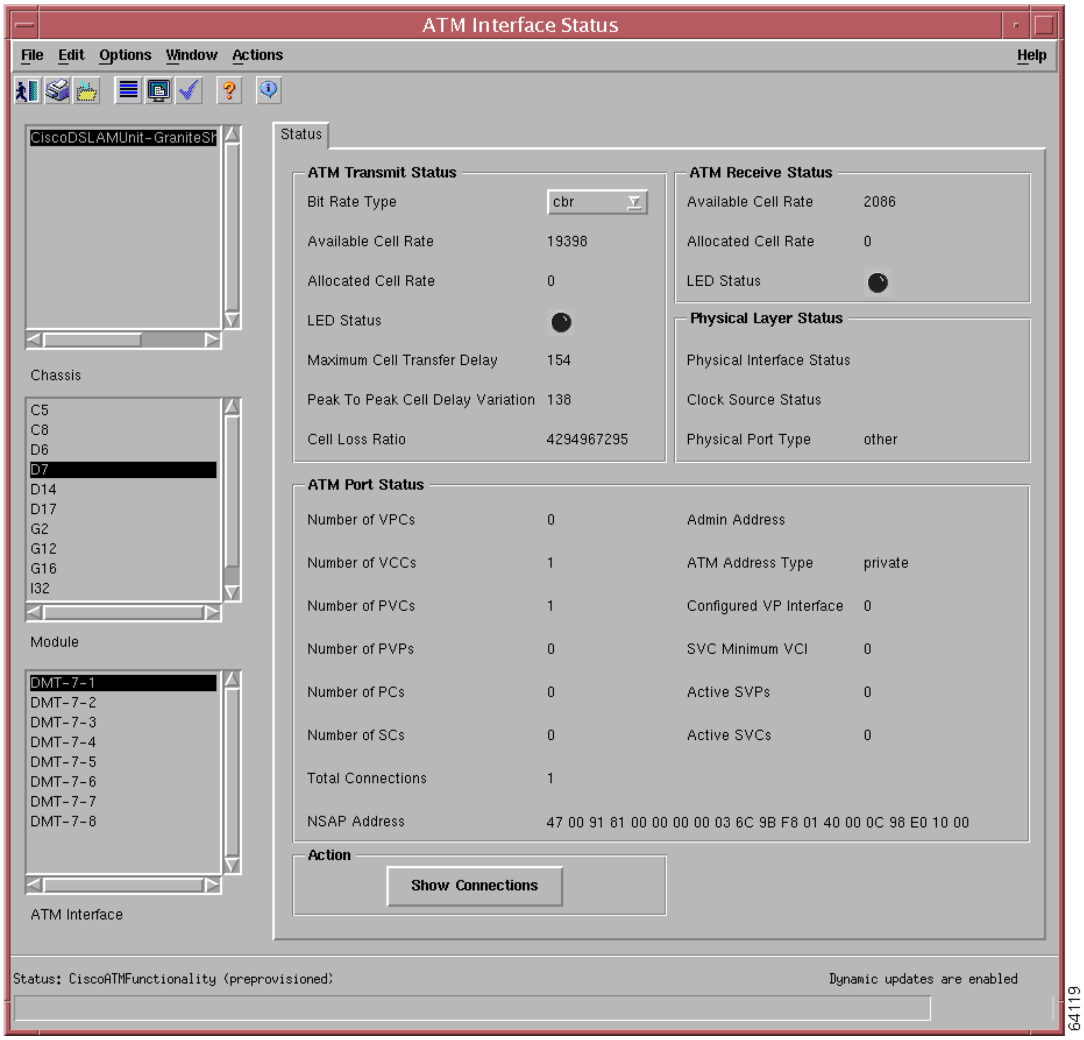
The ATM Interface Status window displays status information for a selected ATM interface. To open the ATM Interface Status window, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click either an NI-2 card or a line card whose ATM status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > ATM** from the object menu.

The ATM Interface Status window opens. The ATM Interface Status window has one tab, the Status tab. (See Figure 7-5.)

Figure 7-5 ATM Interface Status Window



The chassis and interface that you selected is highlighted in the list boxes on the left side of the window. If not, click the appropriate interface from the list box on the left to highlight it. The relevant ATM interface status displays in the Status tab on the right. The Status tab contains five areas:

- ATM Transmit Status
- ATM Receive Status
- Physical Layer Status
- ATM Port Status
- Action

The fields in this window are described in Table 7-5.

Note The interfaces listed in the ATM Interface list box are DMT, ATM, and ADSL interfaces.

Table 7-5 ATM Interface Status—Status Tab Field Descriptions

Field	Description
ATM Transmit Status	
Bit Rate Type	Specifies the service category.
Available Cell Rate	Indicates the available cell rate, specified in cells per second, for traffic that is sent out through the interface for this service category. This value is the bandwidth available for connections. For guaranteed service categories, this value decreases as a result of connection setup and increases as a result of connection release. For nonguaranteed service categories, this value does not change as a result of connection setup and connection release.
Allocated Cell Rate	Indicates the allocated cell rate, specified in cells per second, for traffic that is sent out the interface for this service category. This value is the bandwidth that is allocated to connections. For guaranteed service categories, this value increases as a result of connection setup and decreases as a result of connection release. For nonguaranteed service categories, this value is always 0.
LED Status	Indicates the transmit LED color for the selected port.
Maximum Cell Transfer Delay	Indicates the maximum cell transfer delay estimated to be experienced by cells of connections transmitted out this interface or this service category.
Peak To Peak Cell Delay Variation	Indicates the estimated peak to peak cell delay variation for cells of this service category that are transmitted out of this interface.
Cell Loss Ratio	Indicates the estimated cell loss ratio for cells of this service category that are transmitted out of this interface.
ATM Receive Status	
Available Cell Rate	Indicates the available cell rate, specified in cells per second, for traffic that is received by the interface for this service category. This value is the bandwidth that is available for connections. For guaranteed service categories, this value decreases as a result of connection setup and increases as a result of connection release. For nonguaranteed service categories, this value does not change as a result of connection setup and connection release.
Allocated Cell Rate	Indicates the allocated cell rate, specified in cells per second, for traffic that is received by the interface for this service category. This value is the bandwidth allocated to connections. For guaranteed service categories, this value increases as a result of connection setup and decreases as a result of connection release. For nonguaranteed service categories, this value is always 0.
LED Status	Indicates the receive LED color for the selected port.

Table 7-5 ATM Interface Status—Status Tab Field Descriptions (continued)

Field	Description
Physical Layer Status	
Physical Interface Status	Not used.
Clock Source Status	Not used.
Physical Port Type	Indicates the physical layer medium on the port. The type is one of the following port types: • other • cpu • Ethernet • OC-3 Utp • OC-3 single-mode fiber • OC-3 multimode fiber • OC-12 single-mode fiber • DS3 • E3
ATM Port Status	
Number of VPCs	Displays the number of VPCs (PVCs and SVCs) that are configured for use at this ATM interface. At the ATM UNI, the configured number of VPCs (PVCs and SVCs) can range from 0 to 256 only.
Number of VCCs	Displays the number of VCCs (PVCs and SVCs) that are configured for the ATM interface.
Number of PVCs	Displays the number of PVCs at this interface.
Number of PVPs	Displays the number of permanent virtual paths at this interface.
Number of PCs	Displays the number of permanent connections (virtual channels or virtual paths) of this service category that are currently allocated to the interface.
Number of SCs	Displays the number of signalled connections (virtual channels or virtual paths) of this service category that are currently allocated to the interface.
Total Connections	Displays the number of existing connections at this interface.
Admin Address	Not used.
ATM Address Type	Displays the type of primary ATM address that is configured for use at the ATM interface.
Configured VP Interface	Displays the number of configured VP interfaces at this physical interface.
SVC Minimum VCI	Displays the minimum value in the range of values from which VCIs are assigned to new SVCs. As this value increases, the number of VCIs that are available for PVCs increases. This value applies to each VPI of the physical interface and each logical port.
Active SVPs	Displays the number of active, switched virtual paths at this interface.

Table 7-5 ATM Interface Status—Status Tab Field Descriptions (continued)

Field	Description
Active SVCs	Displays the number of active, switched virtual connections at this interface.
NSAP[1] Address	Displays the NSAP address.
Action	
Show Connections button	Click to instruct CDM to identify the connections that are currently configured for the selected interface. An action log opens that lists all connections that CDM found on the selected interface. **Note** You must have passwords set for this function to work.

1. NSAP = network service access point

Viewing IMA Group and Link Status on Cisco 6015, 6160, and 6260 DSLAMs

The IMA Group Status window displays the status data for IMA groups. The IMA Link Status window displays status information about the IMA links. These windows are described in the following sections:

- Viewing the IMA Group Status Window, page 7-14
- Viewing the IMA Link Status Window, page 7-17

Viewing the IMA Group Status Window

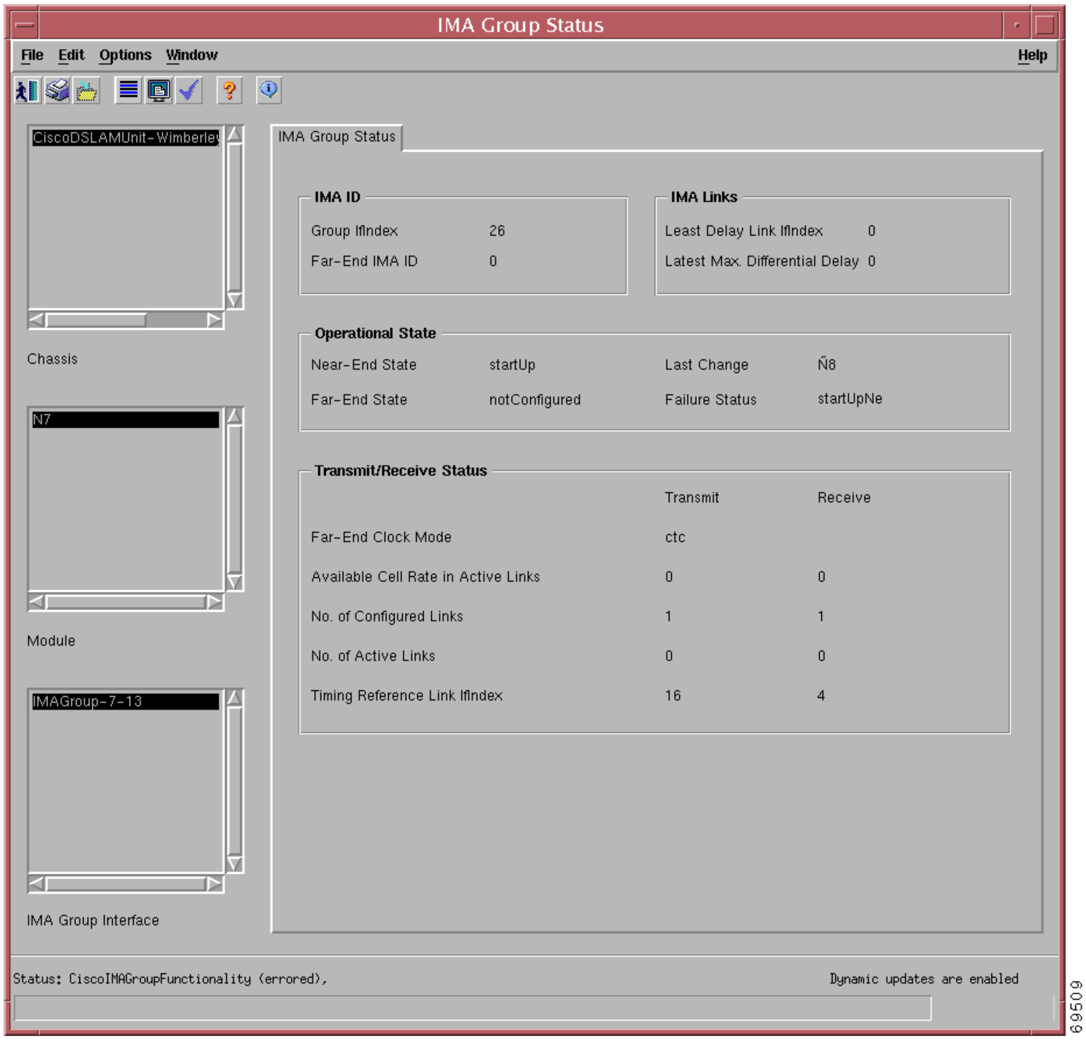
Complete the following steps to open the IMA Group Status window and view status about the IMA group settings:

Step 1 From the left side of the Map Viewer window, from within the Component Managed or the IMA hierarchy view, right-click the NI card or IMA group whose status you want CDM to display.

Step 2 Choose **Cisco DSL Manager > Interface > Status > IMA Group** from the object menu.

The IMA Group Status window opens. (See Figure 7-6.)

Figure 7-6 IMA Group Status Window



This window contains the following areas:

- IMA ID
- IMA Links
- Operational State
- Transmit/Receive Status

Step 3 From the Module list box on the left, click the NI card whose IMA group status you want to view if that NI card is not already highlighted.

The fields in the IMA Group Status window are described in Table 7-6.

Table 7-6 IMA Group Status Window Field Descriptions

Field	Description
IMA ID	
Group Ifindex	Displays the interface index for the IMA group.
Far-End IMA ID	Specifies the far-end IMA group ID.
IMA Links	
Least Delay Link Ifindex	Specifies the interface index of the link that is configured in the IMA group and has the smallest link propagation delay. The distinguished value of zero may be used if no link has been configured in the IMA group, or if the link with the smallest link propagation delay has not yet been determined.
Latest Max Differential Delay	Displays the latest maximum differential delay (in milliseconds) that the network observes between the links that have the least and most link propagation delay, among the receive links that are currently configured in the IMA group.
Operational State	
Near-End State	Displays the current state of the near-end transmit link.
Far-End State	Displays the current state of the far-end transmit link.
Last Change	Not used.
Failure Status	Displays the local failure status of a link belonging to an IMA group.
Transmit/Receive Status	
Far-End Clock Mode	Displays the transmit clocking mode—Transmit or Receive—that the far-end IMA group is using.
Available Cell Rate in Active Links	Displays in two columns—Transmit or Receive—the current cell rate (truncated value in cells per second) that this IMA group provides in the transmit or receive direction, considering all the transmit links in the Active state.
No. of Configured Links	Displays in two columns—Transmit or Receive—the number of links that are configured to transmit or receive in this IMA group.

Table 7-6 IMA Group Status Window Field Descriptions (continued)

Field	Description
No. of Active Links	Displays in two columns—Transmit or Receive—the number of links that are configured to transmit or receive and are currently Active in this IMA group.
Timing Reference Link Ifindex	Displays in two columns—Transmit or Receive—the following values: • The interface index of the transmit timing reference link to be used by the near end for IMA data cell clock recovery from the ATM layer. The distinguished value of zero may be used if no link has been configured in the IMA group, or if the transmit timing reference link has not yet been selected. • The interface index of the receive timing reference link to be used by the near end for IMA data cell clock recovery toward the ATM layer. The distinguished value of zero may be used if no link has been configured in the IMA group, or if the receive timing reference link has not yet been detected.

Viewing the IMA Link Status Window

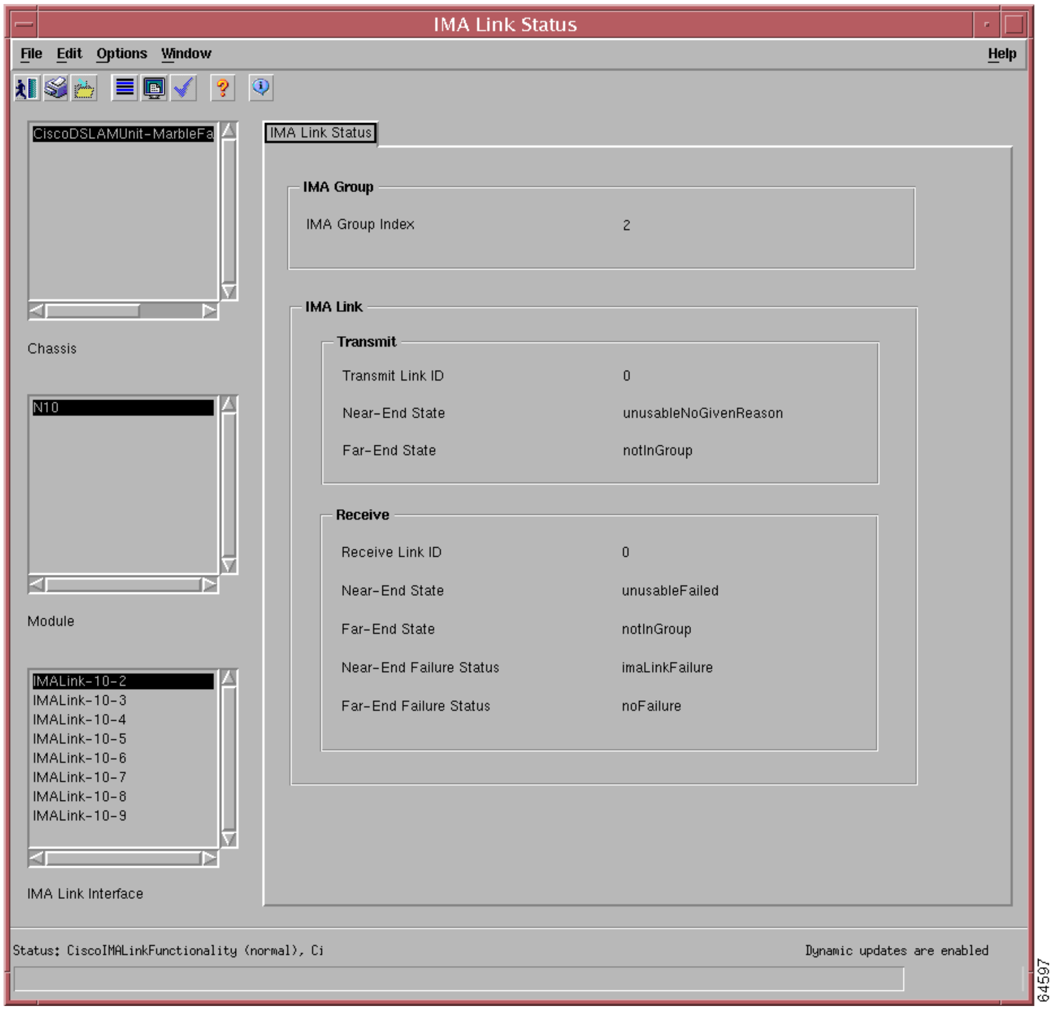
Complete the following steps to open the IMA Link Status window and view status about the IMA group settings:

Step 1 From the left side of the Map Viewer window, from within the IMA hierarchy or the Component Managed view, right-click the NI card or IMA link whose status you want CDM to display.

Step 2 Choose **Cisco DSL Manager > Interface > Status > IMA Link** from the object menu.

The IMA Group Link Status window opens. (See Figure 7-7.)

Figure 7-7 IMA Link Status Window



This window contains the following areas:

- IMA Group
- IMA Link—Transmit and Receive

Step 3 From the Module list box on the left, click the NI card whose IMA link status you want to view if that NI card is not already highlighted.

The fields in the IMA Link Status window are described in Table 7-7.

Table 7-7 IMA Link Status Window Field Descriptions

Field	Description
IMA Group	
IMA Group Index	Specifies a unique value for the IMA group index.
IMA Link—Transmit	
Transmit Link ID	Specifies a unique ID for the transmit link.
Near-End State	Displays the current operational state of the near-end IMA group state machine.
Far-End State	Displays the current operational state of the far-end IMA group state machine.
IMA Link—Receive	
Receive Link ID	Specifies a unique ID for the receive link.
Near-End State	Displays the current operational state of the near-end IMA group state machine.
Far-End State	Displays the current operational state of the far-end IMA group state machine.
Near-End Failure Status	Displays the current link failure status of the near-end receive link.
Far-End Failure Status	Displays the current link failure status of the far-end receive link as reported via ICP cells.

Viewing ADSL Interface Status

This section includes the following topics:

- Viewing the ADSL Interface Status Window—Line Tab, page 7-21
- Viewing the ADSL Interface Status Window—Channel Tab, page 7-22

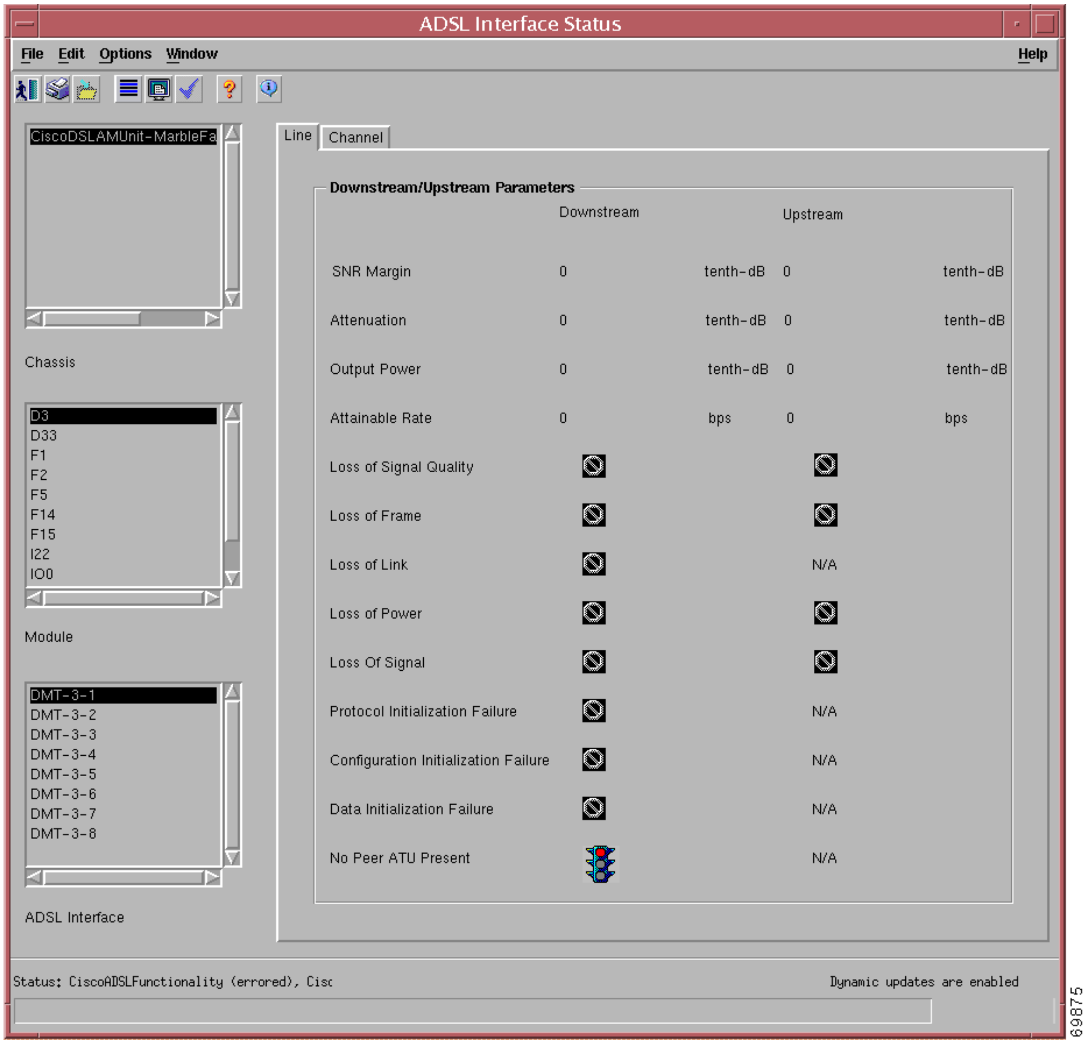
The ADSL Interface Status window displays status information for a selected ADSL line card. To open the ASDL Interface Status window, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the ADSL line card whose interface status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > XDSL > ADSL** from the object menu.

The ADSL Interface Status window opens. (See Figure 7-8.) The ADSL Interface Status Window has two tabs—Line and Channel.

Figure 7-8 ADSL Interface Status Window—Line Tab



Step 3 From the list boxes on the left, select the relevant chassis, card, and DMT interface.

The status information for the selected DMT line card displays on the right.

Viewing the ADSL Interface Status Window—Line Tab

The ADSL Interface Status window Line tab displays line status information for the selected line card. The Line tab contains one area—Downstream/Upstream Parameters. The fields in this tab are described in Table 7-8.

Table 7-8 ADSL Interface Status window—Line Tab Field Descriptions

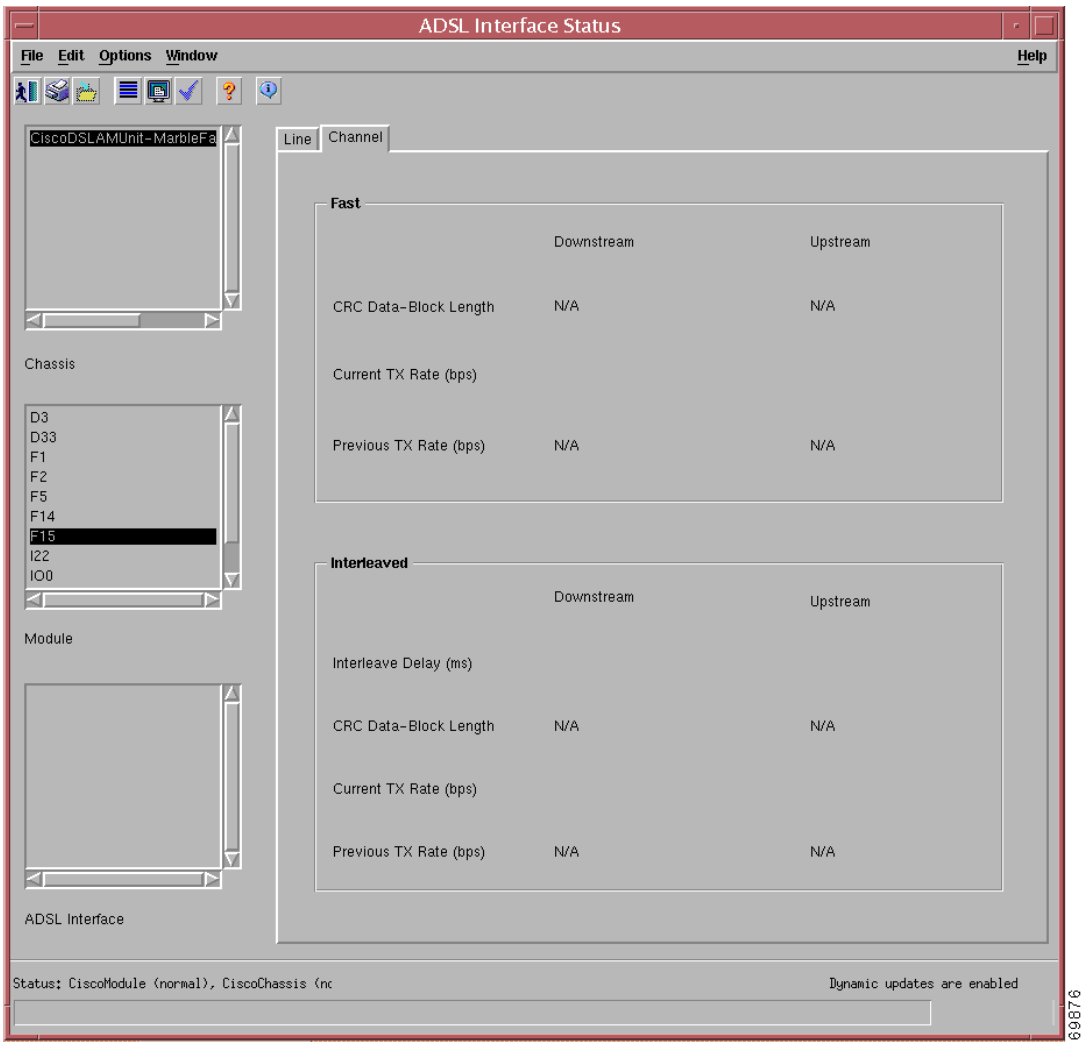
Attribute	Description
SNR Margin	Displays the noise margin as seen by the ATU-C[1] (downstream) and ATU-R[2] (upstream) with respect to its received signal in tenth-dB.
Attenuation	Displays the measured difference in the total power that is being transmitted by the peer ATU and the total power received by this ATU-C (downstream) and ATU-R (upstream) in tenth-dB.
Output Power	Displays the measured total output power that is being transmitted by the ATU-C (downstream) and ATU-R (upstream) in tenth dB.
Attainable Rate	Displays the maximum rate that is currently attainable by the ATU (downstream) and ATU-R (upstream) in bps.
Loss of Signal Quality	Indicates ATU-C (downstream) and ATU-R (upstream) failure due to loss of signal quality. Loss of signal quality is declared when the noise margin falls below the minimum noise margin, or the bit-error-rate exceeds 10^{-7}.
Loss of Frame	Indicates ATU-C (downstream) and ATU-R (upstream) failure due to not receiving a valid frame.
Loss of Link	Indicates ATU-C failure due to inability to link with the ATU-R.
Loss of Power	Indicates ATU-C (downstream) and ATU-R (upstream) failure due to a loss of power.
Loss of Signal	Indicates ATU-C (downstream) and ATU-R (upstream) failure due to a loss of signal.
Protocol Initialization Failure	Indicates ATU-C failure during initialization due to incompatible protocol used by the peer ATU.
Configuration Initialization Failure	Indicates ATU-C failure during initialization due to the peer ATU not being able to support requested configuration.
Data Initialization Failure	Indicates ATU-C failure during initialization due to bit errors that are corrupting the startup exchange data.
No Peer ATU Present	Indicates ATU-C failure during initialization due to no activation sequence detected from peer ATU.

1. ATU-C = ADSL transmission unit - central office
2. ATU-R = ADSL transmission unit - remote

Viewing the ADSL Interface Status Window—Channel Tab

The ADSL Interface Status window Channel tab displays fast and interleaved channel status information for the selected DMT line card. The Channel tab opens includes two areas, Fast and Interleaved. (See Figure 7-9.)

Figure 7-9 ADSL Interface Status Window—Channel Tab



The fields on the ADSL Interface Status window Channel tab are described in Table 7-9.

Table 7-9 ADSL Interface Status Window—Channel Tab Field Descriptions

Attribute	Description
Fast	
CRC[1] Data-Block Length	Indicates the length of the channel data block on which the CRC operates.
Current TX Rate (bps)	Displays the actual downstream or upstream data transmission rate on this channel.

Table 7-9 ADSL Interface Status Window—Channel Tab Field Descriptions (continued)

Attribute	Description
Previous TX Rate (bps)	Indicates the rate at the time of the last RateChangeTrap event.
Interleaved	
Interleave Delay (ms)	Indicates the interleave delay for the interleave channel.
CRC Data-Block Length	Indicates the length of the interleave channel data block on which the CRC operates.
Current TX Rate (bps)	Displays the actual downstream or upstream data transmission rate on the interleave channel.
Previous TX Rate (bps)	Indicates the rate at the time of the last RateChangeTrap-Interleave Channel type event.

1. CRC = cyclic redundancy check

Viewing DMT Interface Status

This section includes the following topics:

- Viewing the DMT Interface Status Window—Line Tab, page 7-24
- Viewing the DMT Interface Status Window—Channel Tab, page 7-27

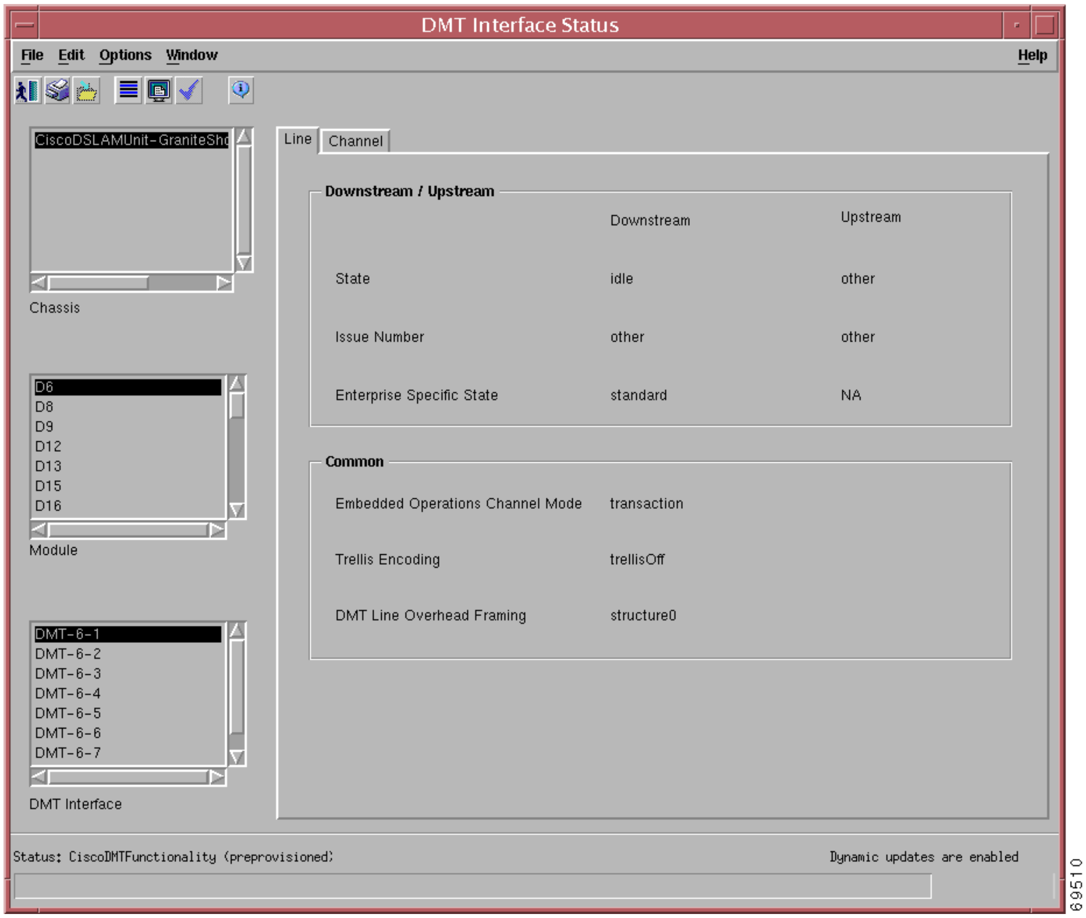
The DMT Interface Status window displays status information for a selected DMT line card. To open the DMT Interface Status window, complete the following steps:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the DMT line card whose interface status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > XDSL > DMT** from the object menu.

The DMT Interface Status window opens. (See Figure 7-10.) The DMT Interface Status Window has two tabs—Line tab and Channel tab.

Figure 7-10 DMT Interface Status Window—Line Tab



Step 3 From the list boxes on the left, select the relevant chassis, card, and DMT interface.

The status information for the selected DMT line card displays on the right.

Viewing the DMT Interface Status Window—Line Tab

The DMT Interface Status window Line tab displays line status information for the selected DMT line card. The Line tab contains two areas—Downstream/Upstream and Common. The fields in this tab are described in Table 7-10.

Table 7-10 DMT Interface Status window—Line Tab Field Descriptions

Attribute	Description
Downstream/Upstream	
State	Indicates the current state of the DMT transceiver. The current state changes dynamically. The possible values displayed for downstream status are as follows: • Other—Unknown or other state • PowerUp—DMT transceiver not yet configured • Configure—DMT transceiver being configured • Idle—Awaiting activation request from upstream • Tone—Requesting upstream to be silent • Activating—Activation in progress • Training—Transceiver training in progress • Analyzing—Channel analysis in progress • Exchange—Exchanging final operating parameters • SteadyState—Normal operating mode • NotResponding—DMT transceiver not responding The possible state values displayed for upstream status are as follows: • Other—Unknown or other state • Activating—Activation in progress • Training—Transceiver training in progress • Analyzing—Channel analysis in progress • Exchange—Exchanging final operating parameters • Steady State—Normal operating mode
Issue Number	Reports the issue number of the standard. The standard is determined by whether the downstream DMT ADSL transceiver is currently operating. The issue number is determined by the hardware and is transmitted by the downstream device in C-MSGS1 during initialization. The upstream device transmits the issue number in an R-MSGS1 message during initialization. The possible issue numbers include: • Other—unknown or other • t1413Issue1—ANSI T1.413 Issue 1 • t1413Issue2—ANSI T1.413 Issue 2 • t1413Issue3—ANSI T1.413 Issue 3 • gdmtIssue1—ITU G.dmt Issue 1 • etsiIssue1—ETSI DMT Issue 1

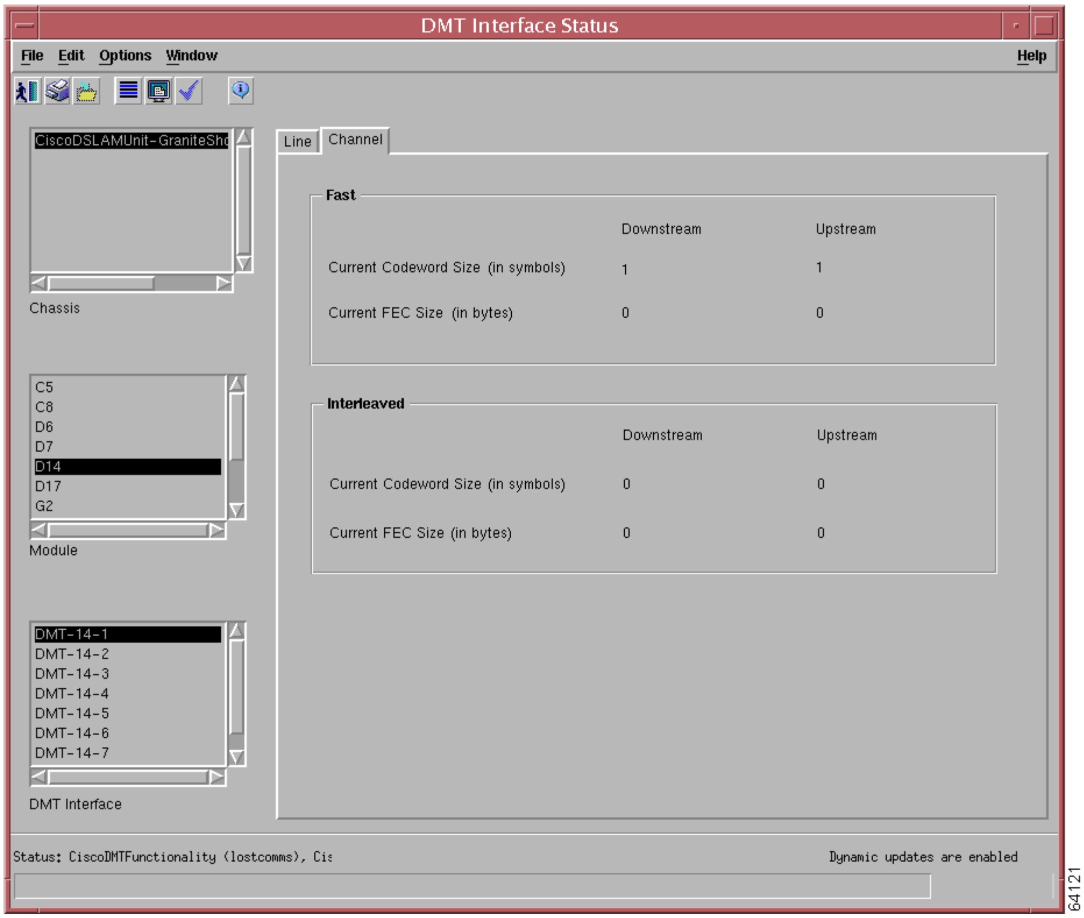
Table 7-10 DMT Interface Status window—Line Tab Field Descriptions (continued)

Attribute	Description
Enterprise Specific State	Specifies the enterprise-specific status of the downstream device, either other or standard. If this field displays other and the downstream device is unrecognized, this status is unknown. If this fields displays other and the downstream device is recognized, this status specifies the enterprise-specific state of the downstream device.
Common	
Embedded Operations Channel Mode	Reports whether the embedded operations channel can support autonomous data streaming mode or only transaction mode. After initialization, unknown is reported until sufficient autonomous eoc messages transmit to determine the true capability of both ATUs. The possible values displayed and the corresponding meaning are as follows: • Unknown—Embedded operations mode is unknown • Transaction—Embedded operations channel only operates in original transaction mode • Streaming—Embedded operations channel supports autonomous data streaming mode and original transaction mode
Trellis Encoding	Reports whether the DMT line is using trellis coding. Use of trellis coding is determined at line initialization with C-MSGS1 and R-MSGS1 exchanges and does not change until the line is reinitialized. The possible values displayed are as follows: • trellisOn • trellisOff
DMT Line Overhead Framing	Represents the negotiated overhead framing structure being used downstream and upstream from the following possible settings: • 0 = Full Asynchronous. Full-overhead framing with asynchronous bit-to-modem timing (enabled synchronization control mechanism). • 1 = Full Synchronous. Full-overhead framing that uses synchronous bit-to-modem timing, a disabled synchronization control mechanism. • 2 = Reduced Separate Fast. Reduced-overhead framing that has separate fast and sync bytes. Bytes exist in fast and interleaved latency buffer respectively (64 kbps framing overhead). • 3 = Reduced Merged Fast. Reduced overhead framing with merged fast and dsync byte, using either the fast or interleaved latency buffer (32 kbps framing overhead). This is the recommended setting.

Viewing the DMT Interface Status Window—Channel Tab

The DMT Interface Status window Channel tab displays fast and interleaved channel status information for the selected DMT line card. The Channel tab opens includes two areas, Fast and Interleaved. (See Figure 7-11.)

Figure 7-11 DMT Interface Status Window—Channel Tab



The Fast and Interleaved areas have the same information, but for different types of channels. Both areas display the attributes that are described in Table 7-11.

Table 7-11 DMT Interface Status Window Fast and Interleaved Areas

Field	Description
Fast	
Current Codeword Size	Displays the number of symbols per codeword that the downstream device is using for downstream or upstream messages on an fast channel during the training sequence. The downstream device or the upstream device can fall back from this value based on the aggregate data rate achieved during training.

Table 7-11 DMT Interface Status Window Fast and Interleaved Areas

Field	Description
Current FEC Size	Displays the number of FEC[1] redundancy bytes per codeword. The codeword size affects FEC operation.
Interleaved	
Current Codeword Size	Displays the number of symbols per codeword that the downstream device is using for downstream or upstream messages on an interleaved channel during the training sequence. The downstream or the upstream device can fall back from this value based on the aggregate data rate achieved during training.
Current FEC Size	Displays the number of FEC[2] redundancy bytes per codeword. The codeword size and interleave depth affect FEC operation.

1. FEC = forward error correction
2. FEC = forward error correction

Viewing SONET Interface Status

This section includes the following topics:

- Viewing the SONET Interface Status Window—Medium Tab, page 7-30
- Viewing the SONET Interface Status Window—Section Tab, page 7-31
- Viewing the SONET Interface Status Window—Line Tab, page 7-32
- Viewing the SONET Interface Status Window—Path Tab, page 7-33

After you deploy a Synchronous Optical Network (SONET) interface, you can access status information for that interface in the SONET Interface Status window. (See the “Deploying Objects” section on page 2-6 for deployment instructions.)

Note SONET and OC-3 interfaces are the same component.

Note The SONET Interface Status window Virtual Tributary tab is not used.

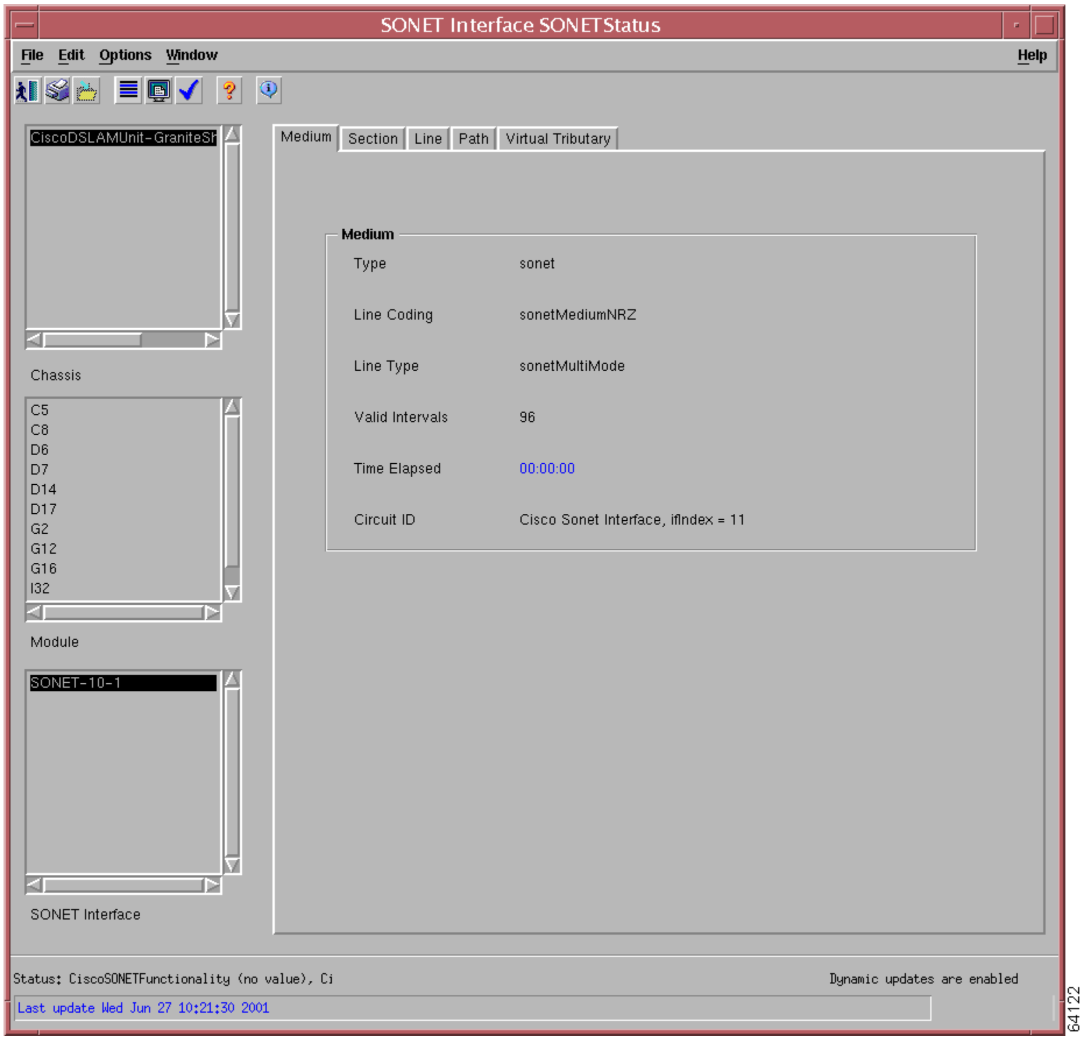
Complete the following steps to view SONET interface status:

Step 1 From the left side of the Map Viewer window, within the Physical view, right-click the NI-2 card whose SONET status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > SONET** from the object menu.

The SONET Interface Status window opens. (See Figure 7-12.)

Figure 7-12 SONET Interface Status Window—Medium Tab



Step 3 From the Module list box on the left, click the NI card whose SONET interface status you want to see.

The window opens to the Medium tab, and the chassis, card, and SONET interface (OC-3 interface) that you selected are highlighted in the list boxes on the left side of the window. The status information for the selected SONET interface displays on the right.

The SONET Interface Status window contains the following tabs:

- Medium
- Section
- Line
- Path
- Virtual Tributary—not used

These tabs are described in the following sections.

Viewing the SONET Interface Status Window—Medium Tab

The Medium tab provides information about the physical medium. The Medium tab contains one area, Medium. The fields in this tab are described in Table 7-12.

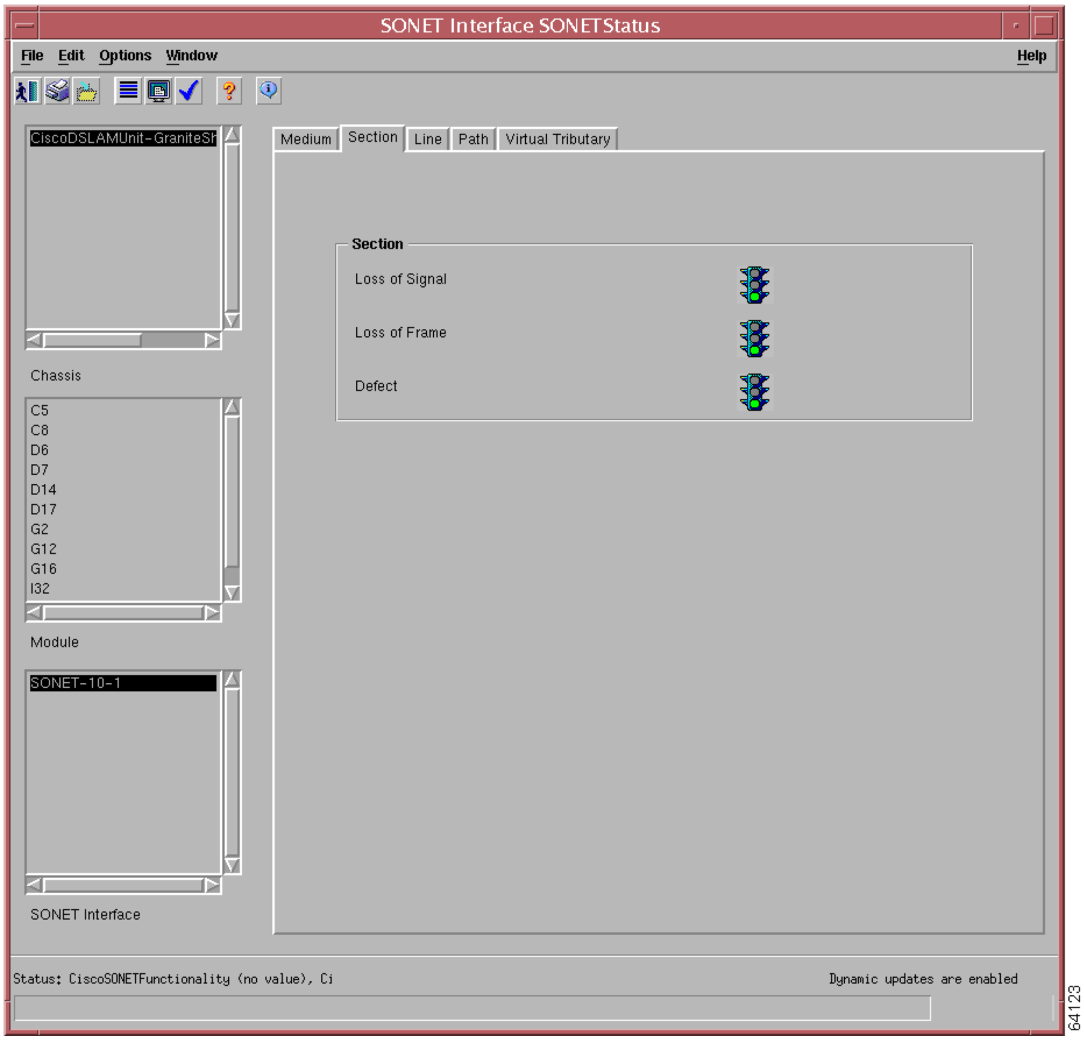
Table 7-12 SONET Interface Status Window—Medium Tab Field Descriptions

Field	Description
Type	Displays SONET to indicate that SONET is operating over the interface.
Line Coding	Displays the type of line coding that the interface is using.
Line Type	Displays the line type of the interface.
Valid Intervals	Displays the number of previous intervals for which valid data has been stored.
Time Elapsed	Displays the time elapsed (in seconds) since the beginning of the current error-measurement period.
Circuit ID	Displays the vendor circuit identifier.

Viewing the SONET Interface Status Window—Section Tab

The SONET Interface Status window Section tab opens, which details errors that the software encounters during framing, scrambling, error monitoring, and section maintenance. The Section tab has one area, Section. (See Figure 7-13.)

Figure 7-13 SONET Interface Status Window—Section Tab



The Section area displays the fields that are described in Table 7-13.

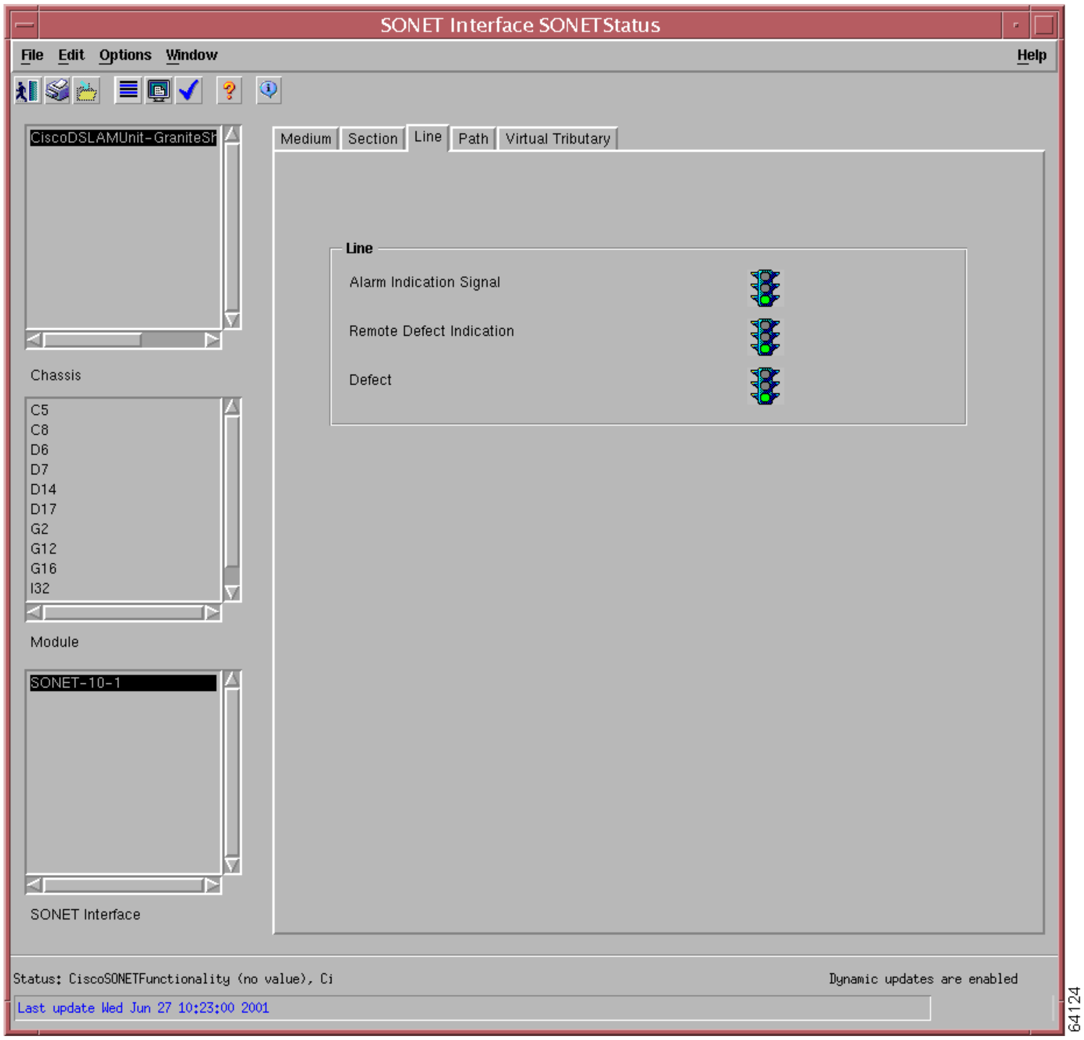
Table 7-13 SONET Interface Status Window—Section Tab Field Descriptions

Field	Description
Loss of Frame	Displays green light to indicate the loss of framing failures since agent reset.
Loss of Signal	Displays green light to indicate the loss of signal failures since agent reset.
Defect or No Defect	Transition from green to red (failure to no alarm state) when no defects (for example, LOF) are received for more than 10 seconds.

Viewing the SONET Interface Status Window—Line Tab

The SONET Interface Status window Line tab opens, which details errors encountered during multiplexing or synchronization. The Line tab has one area, Line. (See Figure 7-14.)

Figure 7-14 SONET Interface Status Window—Line Tab



The Line tab displays the fields that are described in Table 7-14.

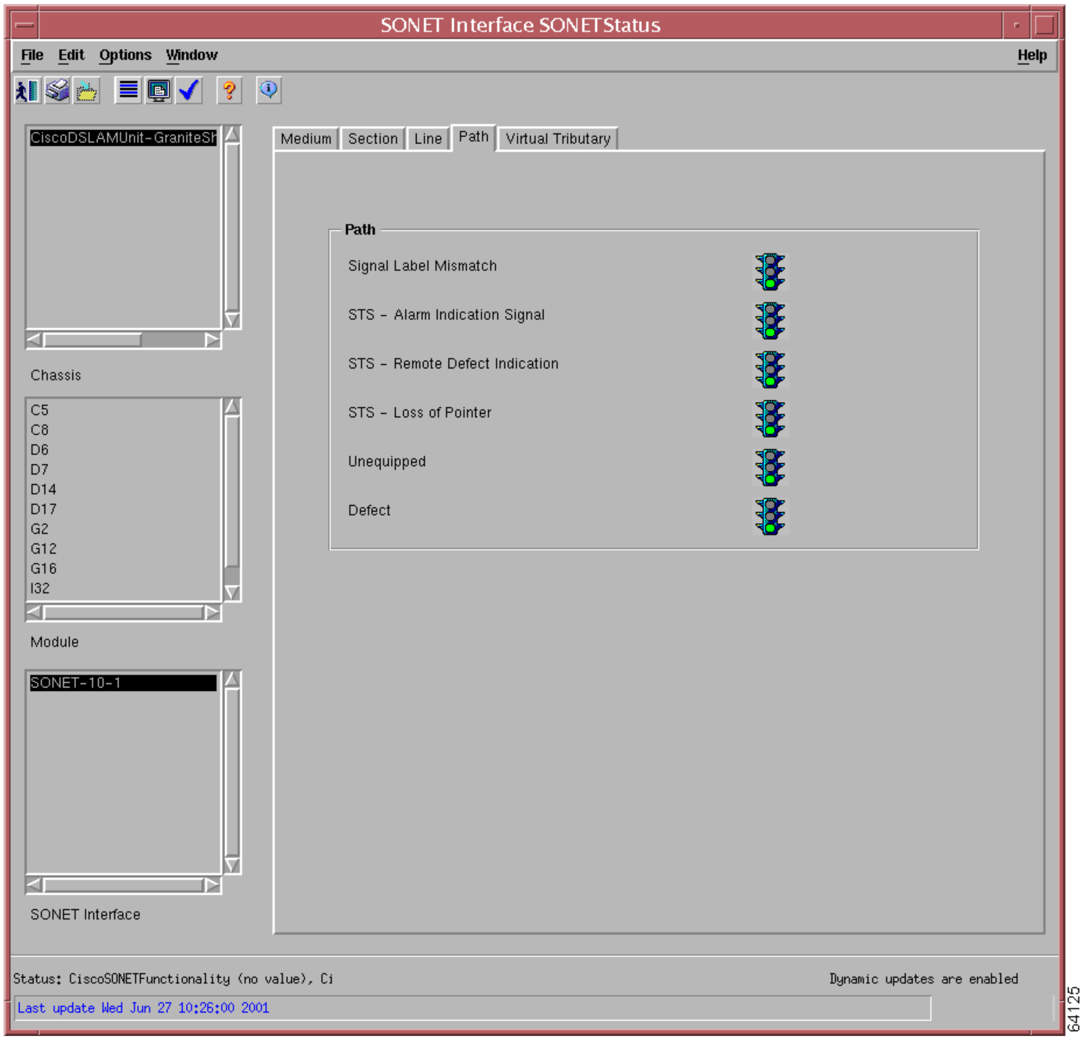
Table 7-14 SONET Interface Window—Line Tab Field Descriptions

Field	Description
Alarm Indication Signal Errors	A green light indicates that line signal errors are detected.
Remote Defect Indication Errors	A green light indicates that remote defect errors have been detected.
Defect or No Defect	Transition from green to red (failure to no alarm state) when no defects (for example, LOF) are received for more than 10 seconds.

Viewing the SONET Interface Status Window—Path Tab

The SONET Interface Status window Path tab opens, which displays errors encountered while mapping signals into the format required by the Line layer. The Path tab has one area, Path. (See Figure 7-15.)

Figure 7-15 SONET Interface Status Window—Path Tab



The fields in this tab are described in Table 7-15.

Table 7-15 SONET Interface Status Window—Path Tab Field Descriptions

Field	Description
Signal Label Mismatch	Displays a green light to indicate incorrect payload type signal label mismatch on a SONET line.
STS—Alarm Indication Signal	Displays a green light to indicate that the path alarm indication signal errors are disabled.
STS—Remote Defect Indication	Displays a green light to indicate that the path remote defect indication errors are disabled.

Table 7-15 SONET Interface Status Window—Path Tab Field Descriptions (continued)

Field	Description
STS—Loss of Pointer	Displays a green light to indicate that the path loss of pointer errors are disabled.
Unequipped	Displays a green light to indicate STS payload unequipped—No path-originating equipment.
Defect or No Defect	Transition from green to red (failure to no alarm state) when no defects (for example, LOF) are received for more than 10 seconds.

Viewing SDSL and G.SHDSL Interface Status

The SDSL Status window displays status information for a selected SDSL or G.SHDSL card. To view the SDSL Status window, follow these steps:

Step 1 In the Map Viewer window, within the Physical view, right-click an SDSL card or a G.SHDSL card whose interface status you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Status > XDSL > SDSL** from the object menu.

The SDSL Status window opens. (See Figure 7-16.)

Figure 7-16 SDSL Interface Status Window

Step 3 Highlight the relevant chassis, card, and SDSL or G.SDSHL interface from the list boxes on the left side of the window.

The status information for the selected SDSL or G.SDSHL line card displays in the window. In the SDSL/G.SHDSL area, the Downstream column applies to both SDSL and G.SHDSL line cards. The Upstream column applies only to G.SHDSL line cards.

Table 7-16 describes the fields that are located in the SDSL Interface Status window. The values in the Downstream column refer to both SDSL and G.SHDSL. The values in the Upstream column relate only the G.SHDSL line cards.

Table 7-16 SDSL Interface Status Window Field Descriptions

Field	Description
SDSL/G.SHDSL	
State	Specifies the state of the STU-C transceiver. Valid values are: • other(1) • idle(2)—Administratively down • training(3)—Transceiver training in progress • steadyState(4)—Nominal mode of operation • testing(5)—Transceiver in loopback or running BERT • downloading(6)—STU-C code download in progress • downloadingFailed(7)—STU-C code download failed
Output Power	Specifies the measured total output power transmitted by this STU-C. This is the measurement that was reported during the last activation sequence.
Rate	Specifies the rate the STU-C transceiver was able to obtain following training.
Defect	Specifies any possible defects currently being exhibited by the STU-C.
Signal/Noise Margin	Specifies the signal/noise margin that this STU-C uses for its receive signal.
Gain	Specifies gain applied to this STU-C receiver.
G.SHDSL	
Power Difference	Displays the measured difference in the total power transmitted by the peer STU-C and the total power received by this STU-C.

Viewing FlexiCAP Interface Status

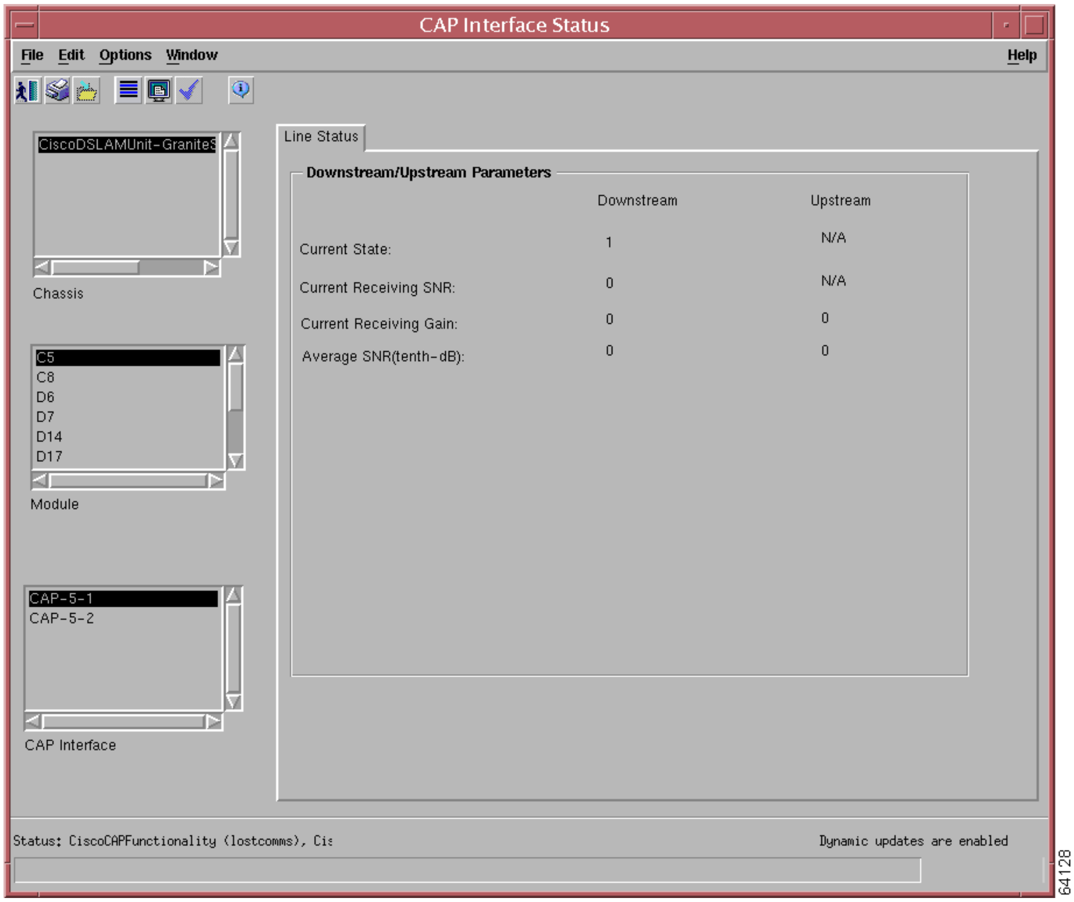
The CAP Interface Status window displays status information for a selected flexiCAP card. To view the CAP Interface Status window, follow these steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the flexiCAP card whose status you want to display.

Step 2 Choose **Cisco DSL Manager > Interface > Status > > XDSL > CAP** from the object menu.

The CAP Interface Status window opens. (See Figure 7-17.)

Figure 7-17 CAP Interface Status Window



The relevant chassis, card, and flexiCAP interface that you selected displays in the list boxes on the left side of the window.

The status information for the selected line card displays on the right.

Table 7-17 describes the fields that are located in the CAP Interface Status Window.

Table 7-17 CAP Interface Status Window Field Descriptions

Field	Description
Current State	Specifies the state of the ATU-C transceiver.
Current Receiving SNR	Specifies the signal-to-noise ratio for the upstream (receive side) data channel.

Table 7-17 CAP Interface Status Window Field Descriptions (continued)

Field	Description
Current Receiving Gain	Specifies the measure of loop attenuation over the entire DSL frequency spectrum. The card uses an algorithm to boost receiver gain so that attenuation can be corrected for proper support of a given receive data rate.
Average SNR (tenth-dB)	Specifies the average signal-to-noise ratio for the upstream (receive side) data channel.

CHAPTER 8

Viewing Performance Data

This chapter describes the interface performance windows in which you can view real-time, current performance information within 10-second polled intervals for interfaces and line cards. This chapter also describes how to access CDM windows that display historical performance data.

This chapter includes the following sections:

Performance polling collects historical data and occurs over a specified time period. Current performance data that you can view on the specific interface performance windows is live; that is, the interface performance windows display what the interface is doing at that moment.

Viewing Current Performance Data in the Interface Performance Windows

This section describes the interface performance windows that are specific to an interface and that display current, live data for that interface. This section includes the following topics:

Viewing CPU Performance Data of NI Cards

You can see how busy the CPU of an NI card is at any given time in the Module Performance window. For example, you may be issuing a lot of SNMP read/write operations on a particular chassis. The load on the CPU of the NI card for that chassis immediately increases; this load on the CPU is reflected in the Module Performance window.

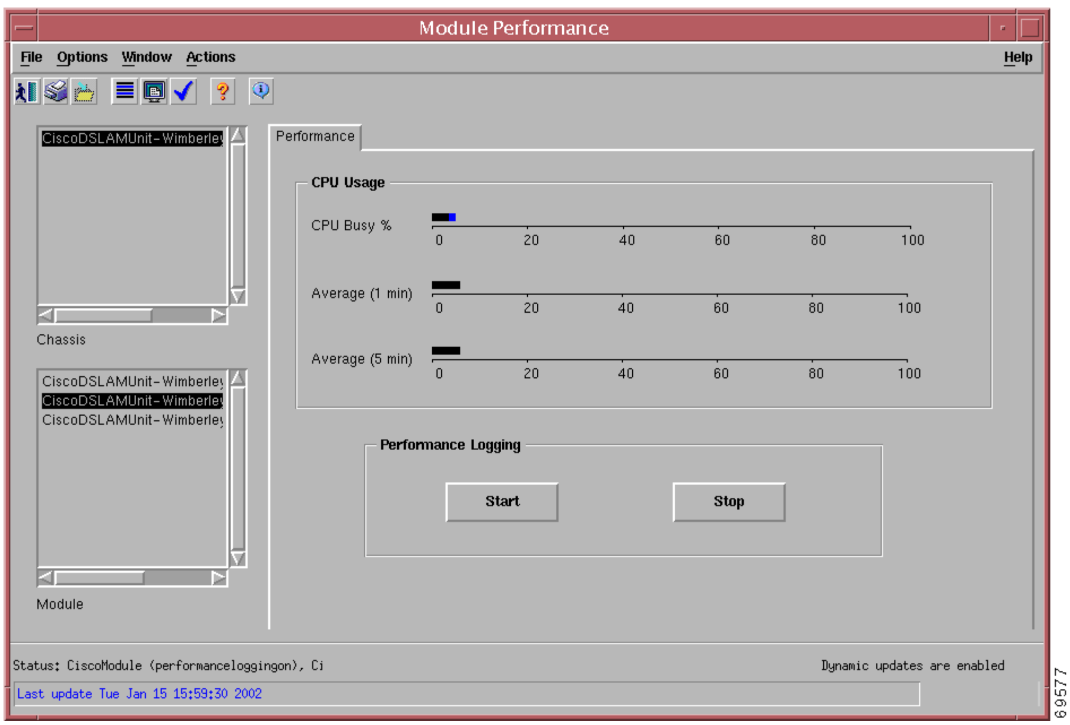
Complete the following steps to open the Module Performance window:

Step 1 From the Physical view, right-click the NI card whose CPU performance you want to view to access the object menu.

Step 2 Choose **Cisco DSL Manager > Module > CPU Performance**.

The Module Performance window opens. (See Figure 8-1.)

Figure 8-1 Module Performance Window



Step 3 Click **Start** in the Performance Logging area to initiate performance logging; click **Stop** to end performance logging.

The Module Performance window displays the same information as the IOS command:

sh processes | include CPU

The Module Performance window has one tab, Performance. The CPU Usage area displays the following information about the NI card CPU.

- CPU Busy %—Displays the current CPU usage.
- Average (1 min)—CPU usage averaged over last 1 minute.
- Average (5 min)—Displays the CPU usage averaged over last 5 minutes.

Viewing *x*DSL Interface Performance Data

The Interface Performance window displays generic performance data for the selected interface. This section applies to viewing line card interface performance data for interfaces such as FlexiDMT and FlexiCAP.

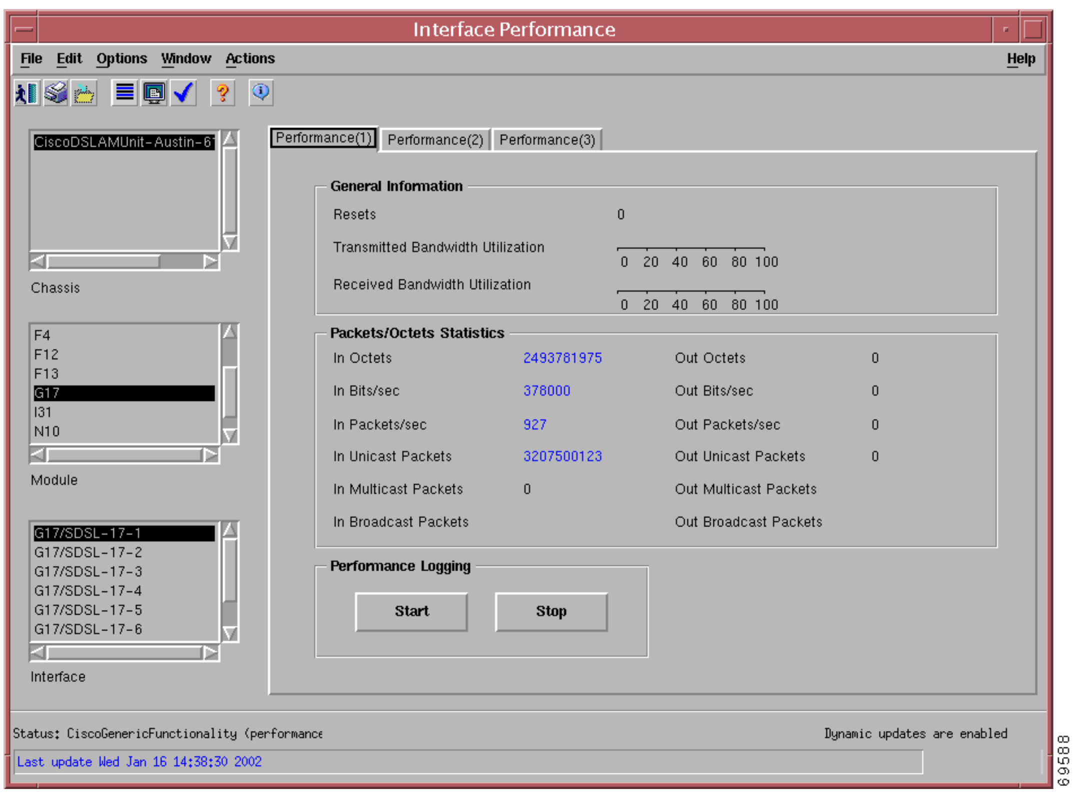
To open the Interface Performance window, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the chassis for which you want to view interface performance data.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > XDSL > Generic** from the object menu.

The Interface Performance window opens to the Performance (1) tab. (See Figure 8-2.)

Figure 8-2 Interface Performance Window—Performance (1) Tab



The chassis, card, and interface that you selected is highlighted in the list boxes on the left side of the window.

The interface performance information for the selected interface displays on the right.

Step 3 Click **Start** to start performance logging on the selected interface.

Step 4 Click **Yes** in the Confirmation dialog box to begin performance logging.

The Action Report dialog box opens to inform you that performance logging is on.

Step 5 Click **Close** to close the Action Report dialog box.

Note Performance logging logs data that displays in the Performance Manager window.

Step 6 Click **Stop** in the Interface Performance window to stop global performance logging.

Step 7 Click **Yes** in the Confirmation dialog box to stop performance logging.

Tip After you have clicked the Stop or Start button, you cannot click that button again.

The Performance (1) tab displays three areas—General Information, Packets/Octets Statistics, and Performance Logging. The fields in this tab are described in Table 8-1.

Table 8-1 Interface Performance Window—Performance (1) Tab Field Descriptions

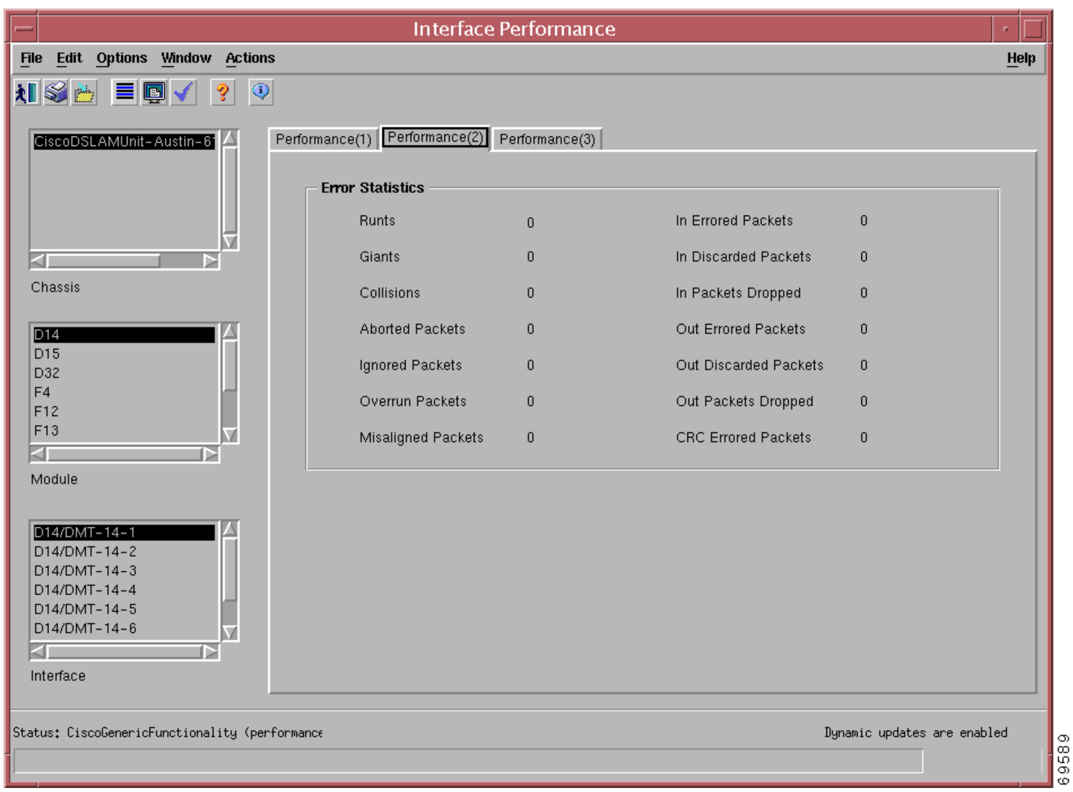
Field	Description
General Information	
Resets	Displays the number of times the interface resets internally.
Transmitted Bandwidth Utilization	Displays the percentage of the bandwidth for transmitting data that is being used.
Received Bandwidth Utilization	Displays the percentage of the bandwidth for receiving data that is being used.
Packets/Octets Statistics	
In Octets	Displays the total number of packets received on the interface, including framing characters.
In Bits/sec	Displays the average number of bits per second received during the last 5-minute period.
In Packets/sec	Displays the average number of packets per second received during the last 5-minute period.
In Unicast Packets	Displays the number of packets received by the layer that were not addressed as multicast or broadcast packets.
In Multicast Packets	Displays the number of packets received by the layer addressed as multicast.
In Broadcast Packets	Displays the number of packets received by the layer addressed as broadcast.
Out Octets	Displays the total number of packets transmitted out of the interface, including framing characters.

Table 8-1 Interface Performance Window—Performance (1) Tab Field Descriptions (continued)

Field	Description
Out Bits/sec	Displays the average number of bits per second transmitted during the last 5-minute period.
Out Packets/sec	Displays the average number of packets per second transmitted during the last 5-minute period.
Out Unicast Packets	Displays the number of packets transmitted by the layer that were not addressed as multicast or broadcast packets.
Out Multicast Packets	Displays the number of packets transmitted by the layer addressed as multicast packets.
Out Broadcast Packets	Displays the number of packets transmitted by the layer addressed as broadcast packets.
Performance Logging	
Start	Click to start performance logging.
Stop	Click to stop performance logging.

The Interface Performance window Performance (2) tab displays Error Statistics. (See Figure 8-3.)

Figure 8-3 Interface Performance Window—Performance (2) Tab



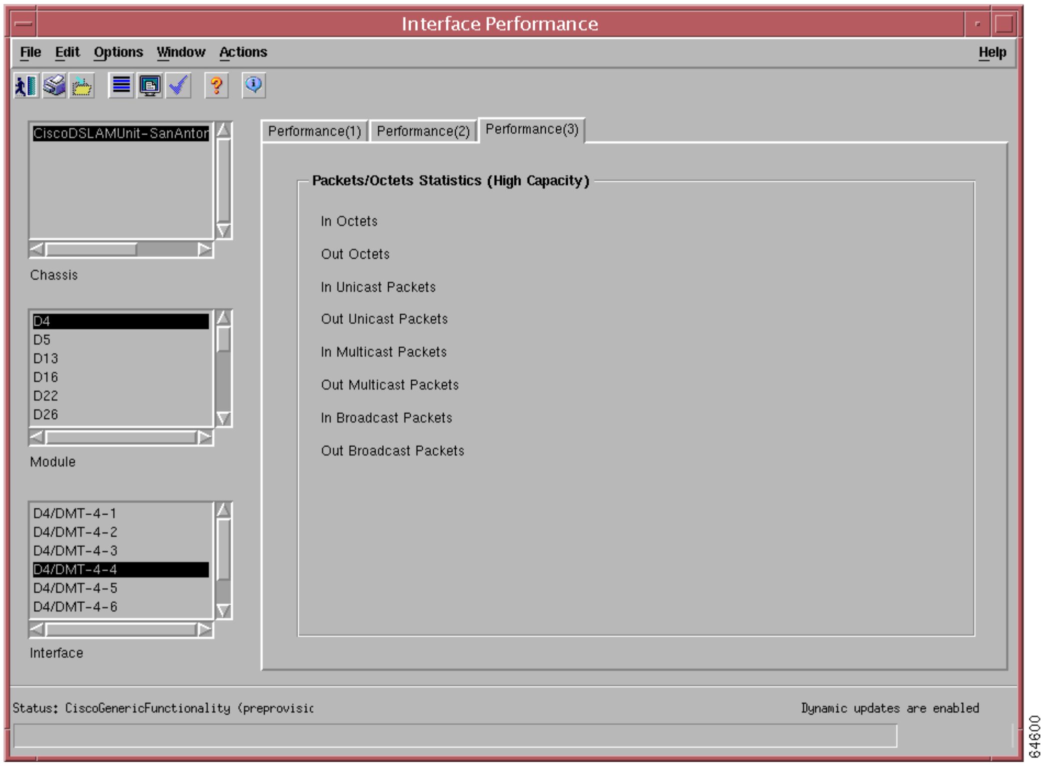
The Performance (2) tab displays a single Error Statistics area; the fields in this area are described in Table 8-2.

Table 8-2 Interface Performance Window—Performance (2) Tab Field Descriptions

Field	Description
Runts	Displays the number of input packets that were smaller than the physical media permits.
Giants	Displays the number of input packets input that were larger than the physical media permits.
Collisions	Displays the number of output collisions detected on this interface.
Aborted Packets	Displays the number of input packets that were aborted.
Ignored Packets	Displays the number of input packets ignored by the selected interface.
Overrun Packets	Displays the number of input packets that arrived too quickly for the hardware to receive.
Misaligned Packets	Displays the number of misaligned input packets.
In Errored Packets	Displays the number of input packets that contained errors.
In Discarded Packets	Displays the number of input packets selected to be discarded even though no errors are found.
In Packets Dropped	Displays the number of packets dropped because the input queue was full.
Out Errored Packets	Displays the number of outbound packets that could not be transmitted because of errors.
Out Discarded Packets	Displays the number of outbound packets selected to be discarded even though no errors were detected.
Out Packets Dropped	Displays the number of outbound packets dropped because the output queue is full.
CRC Errored Packets	Displays the number of input packets that contain cyclic redundancy checksum errors.

The Interface Performance window Performance (3) tab displays Packets/Octets Statistics (High Capacity). This tab is shown in Figure 8-4.

Figure 8-4 Interface Performance Window—Performance (3) Tab



The fields in this tab are described in Table 8-3.

Table 8-3 Interface Performance Window—Performance (3) Tab Field Descriptions

Field	Description
In Octets[1]	Displays the number of in octets.
Out Octets	Displays the number of out octets.
In Unicast[2] Packets	Displays the number of in unicast packets.
Out Unicast Packets	Displays the number of in unicast packets.
In Multicast Packets	Not used.
Out Multicast Packets	Not used.
In Broadcast Packets	Not used.
Out Broadcast Packets	Not used.

1. octet = an eighth-bit byte
2. unicast = point-to-point communication

Viewing ADSL (DMT) Interface Performance Data

This section includes the following topics:

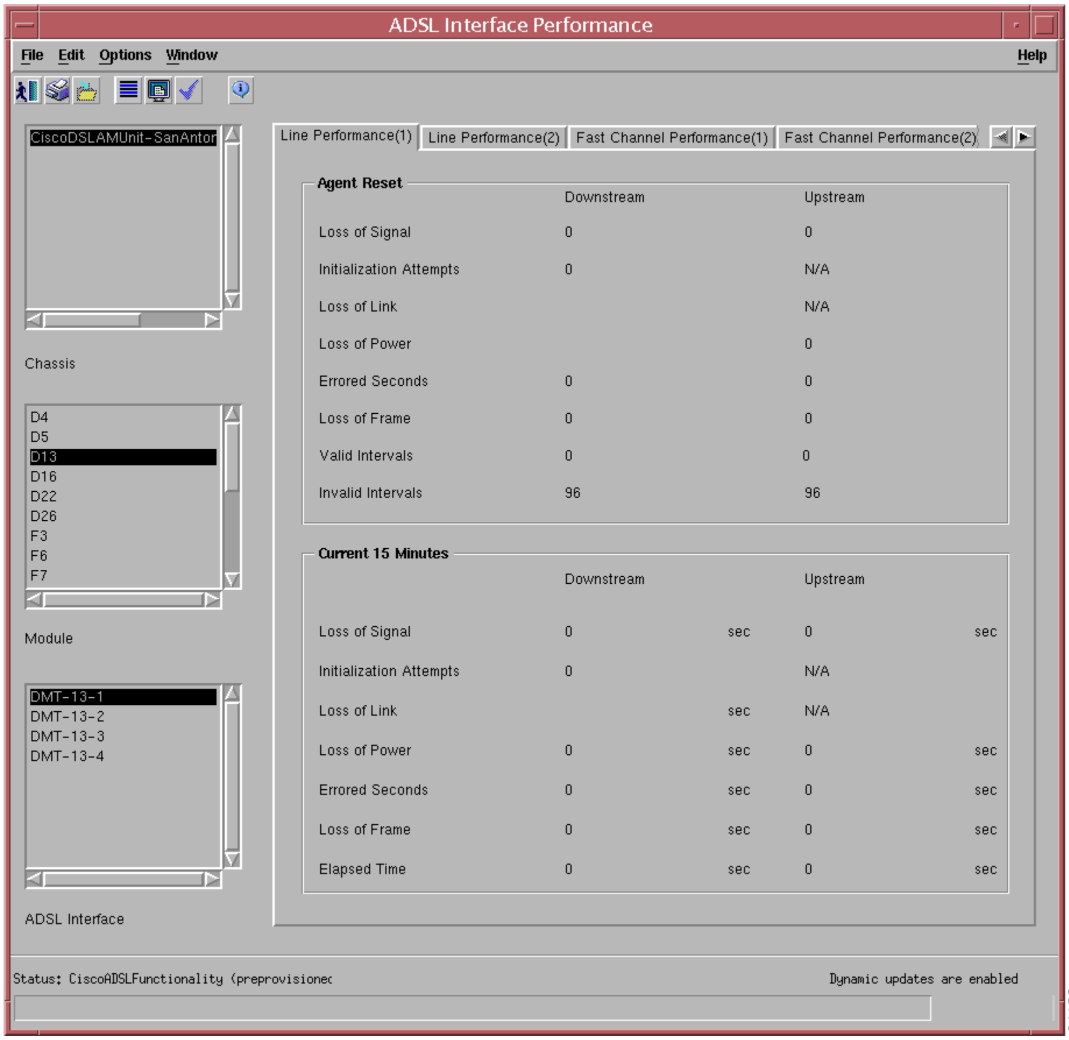
You can view performance data about the ADSL interface in the ADSL Interface Performance window. Complete the following steps to view ADSL performance data:

Step 1 From the Map Viewer window, within the Physical view, right-click the line card whose ADSL performance data you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > XDSL > ADSL** from the object menu.

The ADSL Interface Performance window opens. (See Figure 8-5.)

Figure 8-5 ADSL Interface Performance Window—Line Performance (1) Tab



Note The software automatically creates four DMT interfaces when you deploy a DMT line card. These DMT interfaces are actually ATM over ADSL over DMT interfaces, which means that all three interfaces are combined in CDM and identified by the last specific DMT interface. Therefore, when you view performance information for an ADSL interface, it is identified as a DMT interface.

Step 3 From the list boxes on the left, select the relevant chassis, card, and ADSL interface. The current performance information for the selected ADSL interface appears on the right.

The ADSL Performance window contains six tabs:

- Line Performance (1)
- Line Performance (2)
- Fast Channel Performance (1)
- Fast Channel Performance (2)
- Interleave Channel Performance (1)
- Interleave Channel Performance (2)

The fields in these tabs are described in the following sections.

Viewing the ADSL Interface Performance Window—Line Performance (1) Tab

The Line Performance (1) tab contains two areas—Agent Reset and Current 15 Minutes. These fields are described in Table 8-4.

Note The Agent refers to the Cisco DSLAM chassis.

Note The Current 15 Minutes area displays information collected during the most recent 15-minute interval for which performance monitoring information was derived.

Table 8-4 ADSL Interface Performance Window—Line Performance (1) Tab Field Descriptions

Field	Description
Agent Reset	
Loss of Signal	Displays the total number of loss of signal failures since the last reset.
Initialization Attempts	Displays the total number of line initialization attempts since reset. It includes both successful and failed attempts.
Loss of Link	Displays the number of loss of link failures since reset.
Loss of Power	Displays the number of loss of power failures since reset.
Errored Seconds	Displays the number of errored seconds since reset.
Loss of Frame	Displays the number of loss of framing failures since reset.
Valid Intervals	Displays the number of previous intervals for which valid data has been stored.
Invalid Intervals	Displays the number of previous intervals for which invalid data has been stored.
Current 15 Minutes	
Loss of Signal	Displays the number of seconds in the current 15-minute interval during which loss of signal was detected.
Initialization Attempts	Displays the number of line initialization attempts in the current 15-minute interval. It includes both successful and failed attempts.

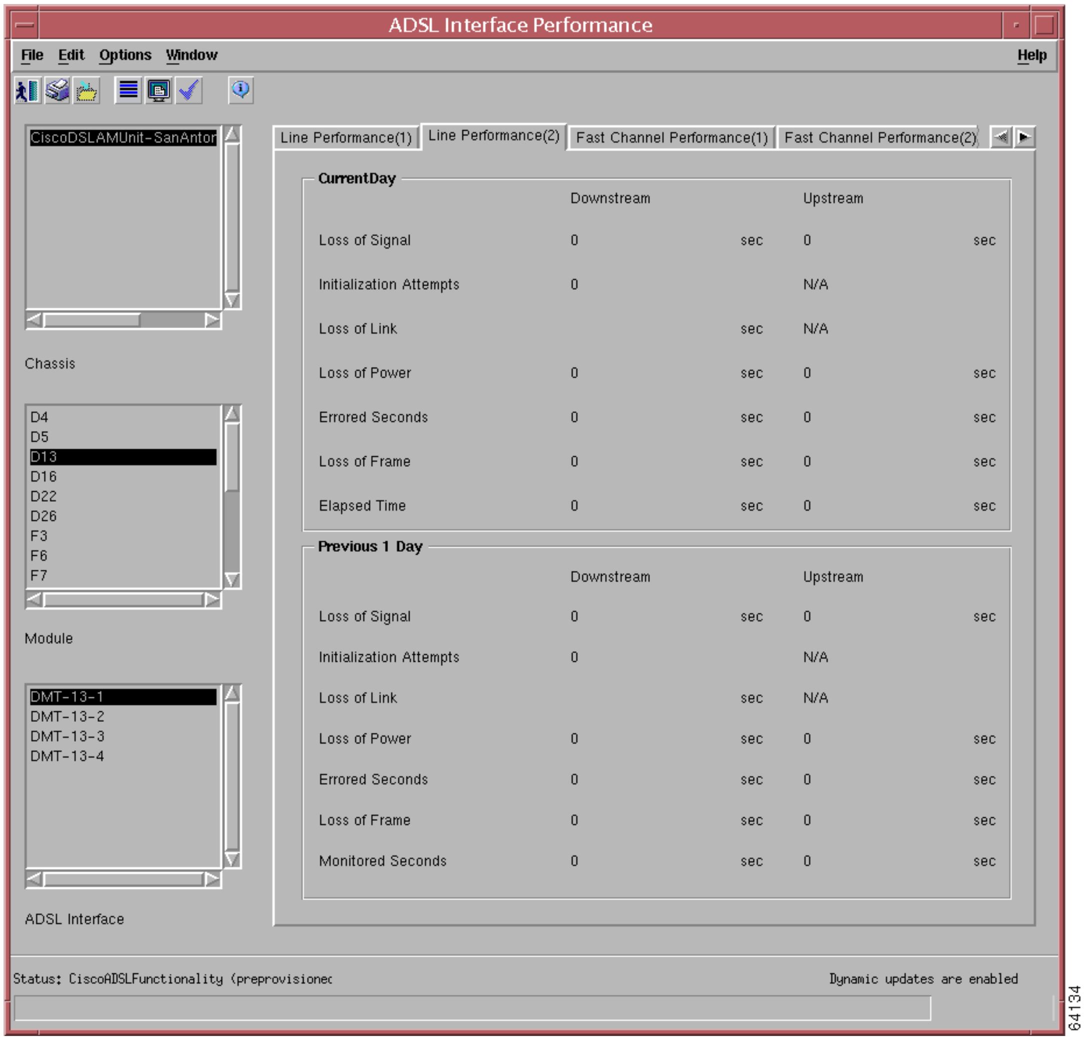
Table 8-4 ADSL Interface Performance Window—Line Performance (1) Tab Field Descriptions (continued)

Field	Description
Loss of Link	Displays the number of seconds in the current 15-minute interval during which loss of link was detected.
Loss of Power	Displays the number of seconds in the current 15-minute interval during which loss of power was detected.
Errored Seconds	Displays the number of errored seconds in the current 15-minute interval.
Loss of Frame	Displays the number of seconds in the current 15-minute interval during which loss of framing was detected.
Elapsed Time	Displays the number of seconds that have elapsed in the specified interval. A full interval is 900 seconds.

Viewing the ADSL Interface Performance Window—Line Performance (2) Tab

The Line Performance (2) tab contains two areas—Current Day and Previous 1 Day. (See Figure 8-6.)

Figure 8-6 ADSL Interface Performance Window—Line Performance (2) Tab



The fields in this tab are described in Table 8-5.

Note The Current Day area displays the time in the current day during which the performance monitoring information is actually counted. This value is normally the same as the total interval duration except in when performance monitoring data cannot be collected.

Note The Previous 1 Day area displays the time in the previous 1-day interval during which the performance monitoring information was actually counted. This value is normally the same as the total interval duration except when performance monitoring data cannot be collected. Typically, elapsed 1-day time is copied into monitored seconds when the 1-day rollover occurs.

Table 8-5 ADSL Interface Performance Window—Line Performance (2) Tab Field Descriptions

Field	Description
Current Day	
Loss of Signal	Displays the number of seconds since there was loss of signal during the current day.
Initialization Attempts	Displays the number of line initialization attempts in the day. It includes both successful and failed attempts.
Loss of Link	Displays the number of seconds since there was loss of link during the current day.
Loss of Power	Displays the number of seconds since there was loss of power during the current day.
Errored Seconds	Displays the number of errored seconds that have elapsed during the current day.
Loss of Frame	Displays the number of seconds since there was loss of framing during the current day.
Elapsed Time	Displays the number of seconds that have elapsed since the beginning of the current 1-day interval.
Previous 1 Day	
Loss of Signal	Displays the number of seconds since there was loss of signal during the previous day.
Initialization Attempts	Displays the number of line initialization attempts in the previous day. It includes both successful and failed attempts.
Loss of Link	Displays the number of seconds over which there was loss of link during the previous day.
Loss of Power	Displays the number of seconds over which there was loss of power during the previous day.
Errored Seconds	Displays the number of errored seconds that have elapsed during the current day.
Loss of Frame	Displays the number of seconds over which there was loss of framing during the previous day.
Monitored Seconds	Displays the number of seconds over which data was collected or monitored during the previous day.

Viewing the ADSL Interface Performance Window—Fast Channel Performance (1) Tab

The Fast Channel Performance (1) tab contains two areas—Agent Reset and Current 15 Minutes. (See Figure 8-7.)

Note An interface is set to either fast channel or interleave, which determines which of these tabs display data. If set to fast channel, the Fast Channel Performance (1) and (2) tabs display data; if set to interleave, the Interleave Channel Performance (1) and (20 tabs display data.

Figure 8-7 ADSL Interface Performance Window—Fast Channel Performance (1) Tab

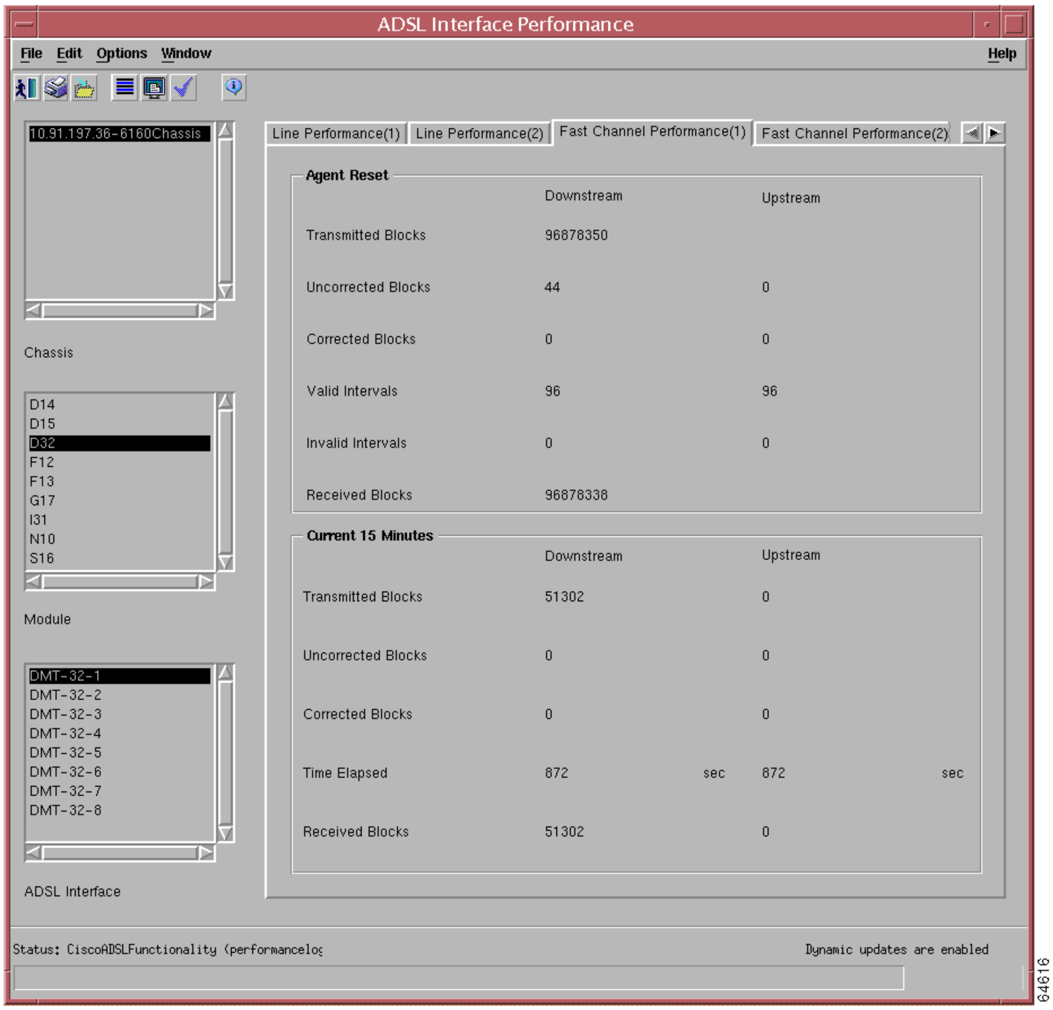


Table 8-6 describes the fields that are in the Fast Channel Performance (1) tab.

Table 8-6 ADSL Interface Performance Window—Fast Channel Performance (1) Tab Field Descriptions

Field	Description
Agent Reset	
Transmitted Blocks	Displays the number of blocks of data transmitted since the last agent reset.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted since the last agent reset.
Corrected Blocks	Displays the number of corrected blocks of data transmitted since the last agent reset.
Valid Intervals	Displays the number of intervals since the last agent reset during which data monitoring was valid.
Invalid Intervals	Displays the number of intervals since the last agent reset during which data monitoring was not valid.
Received Blocks	Displays the number of blocks of data received since the last agent reset.
Current 15 Minutes	
Transmitted Blocks	Displays the number of blocks of data transmitted during the current 15-minute interval.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted during the current 15-minute interval.
Corrected Blocks	Displays the number of corrected blocks of data transmitted during the current 15-minute interval.
Time Elapsed	Displays the amount of time that has elapsed since the start of the current 15-minute interval.
Received Blocks	Displays the number of blocks of data received during the current 15-minute interval.

Viewing the ADSL Interface Performance Window—Fast Channel Performance (2) Tab

The Fast Channel Performance (2) tab contains two areas—Current Day and Previous 1 Day. (See Figure 8-8.)

Figure 8-8 ADSL Interface Performance Window—Fast Channel Performance (2) Tab

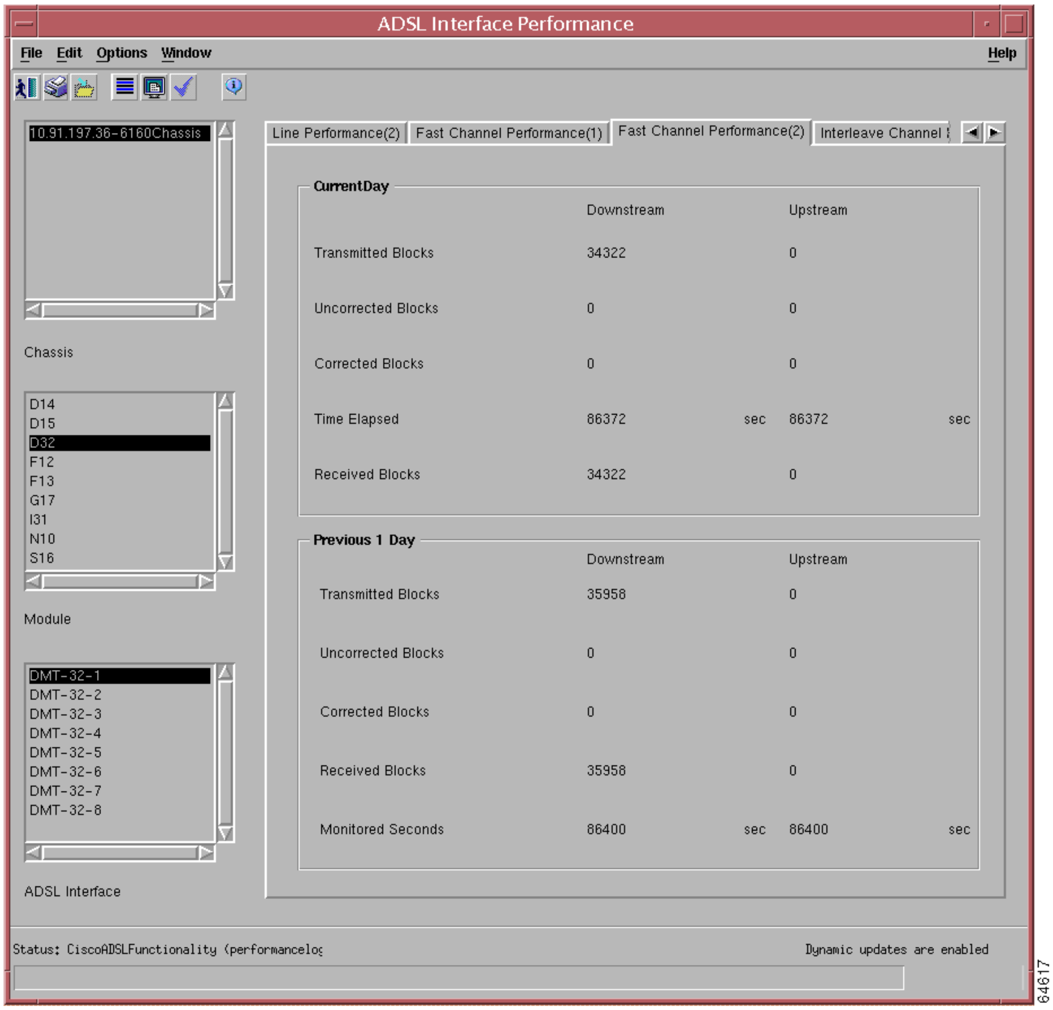


Table 8-7 describes the fields that are in the Fast Channel Performance (2) tab.

Table 8-7 ADSL Interface Performance Window—Fast Channel Performance (2) Tab Attribute Descriptions

Attribute	Description
Current Day	
Transmitted Blocks	Displays the number of blocks of data transmitted during the current day interval.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted during the current day interval.

Table 8-7 ADSL Interface Performance Window—Fast Channel Performance (2) Tab Attribute Descriptions (continued)

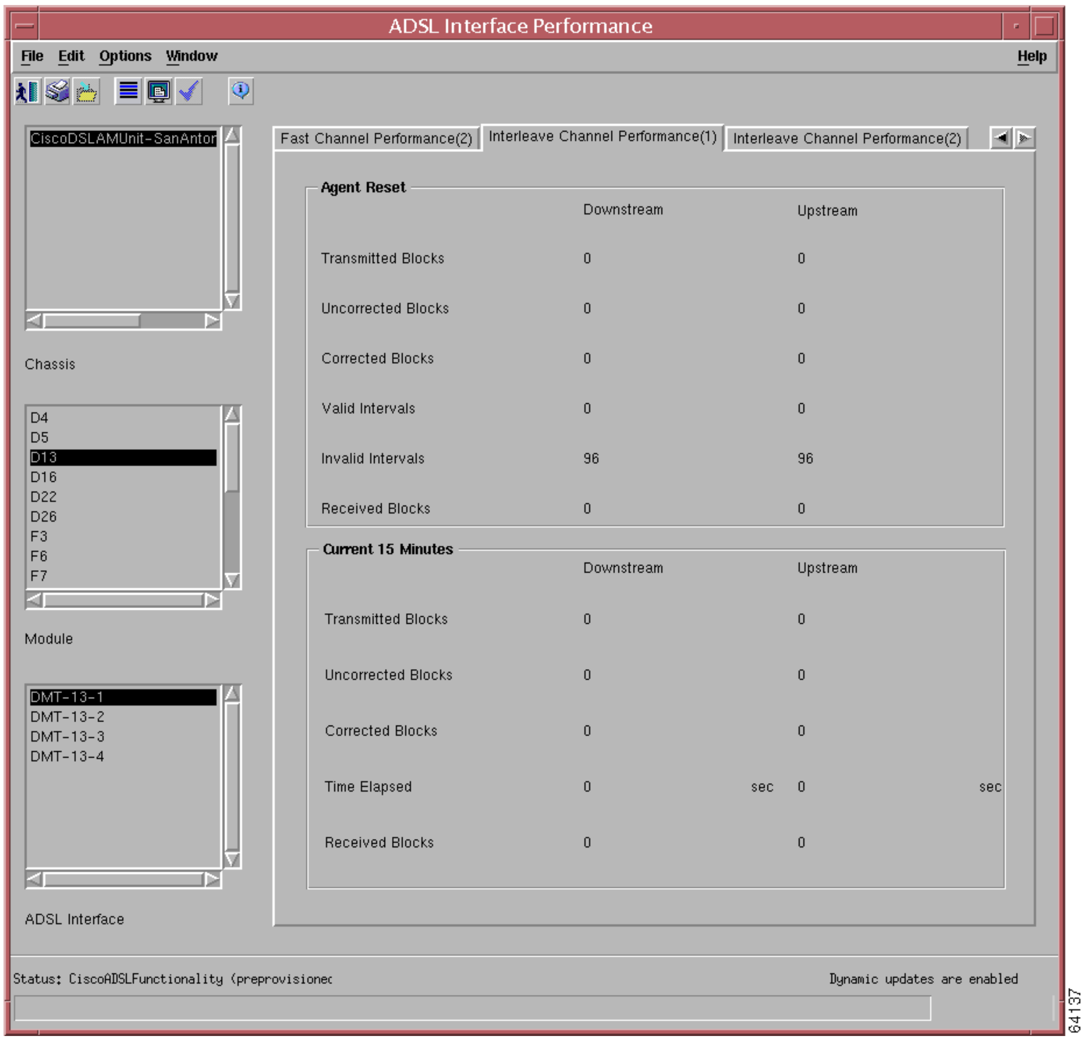
Attribute	Description
Corrected Blocks	Displays the number of corrected blocks of data transmitted during the current day interval.
Time Elapsed	Displays the amount of time that has elapsed since the start of the current day interval.
Received Blocks	Displays the number of blocks of data received during the current day interval.
Previous 1 Day	
Transmitted Blocks	Displays the number of blocks of data transmitted during the previous day interval.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted during the previous day interval.
Corrected Blocks	Displays the number of corrected blocks of data transmitted during the previous day interval.
Received Blocks	Displays the number of blocks of data received during the previous day interval.
Monitored Seconds	Displays the number of seconds during the previous day interval when data was monitored.

Viewing the ADSL Interface Performance Window—Interleave Channel Performance (1) Tab

The Interleave Channel Performance (1) tab contains two areas—Agent Reset and Current 15 Minutes. (See Figure 8-9.)

Note An interface is set to either fast channel or interleave, which determines which of these tabs display data. If set to fast channel, the Fast Channel Performance (1) and (2) tabs display data; if set to interleave, the Interleave Channel Performance (1) and (20 tabs display data.

Figure 8-9 ADSL Interface Performance Window—Interleave Channel Performance (1) Tab



The Interleave Channel Performance (1) tab fields are described in Table 8-8.

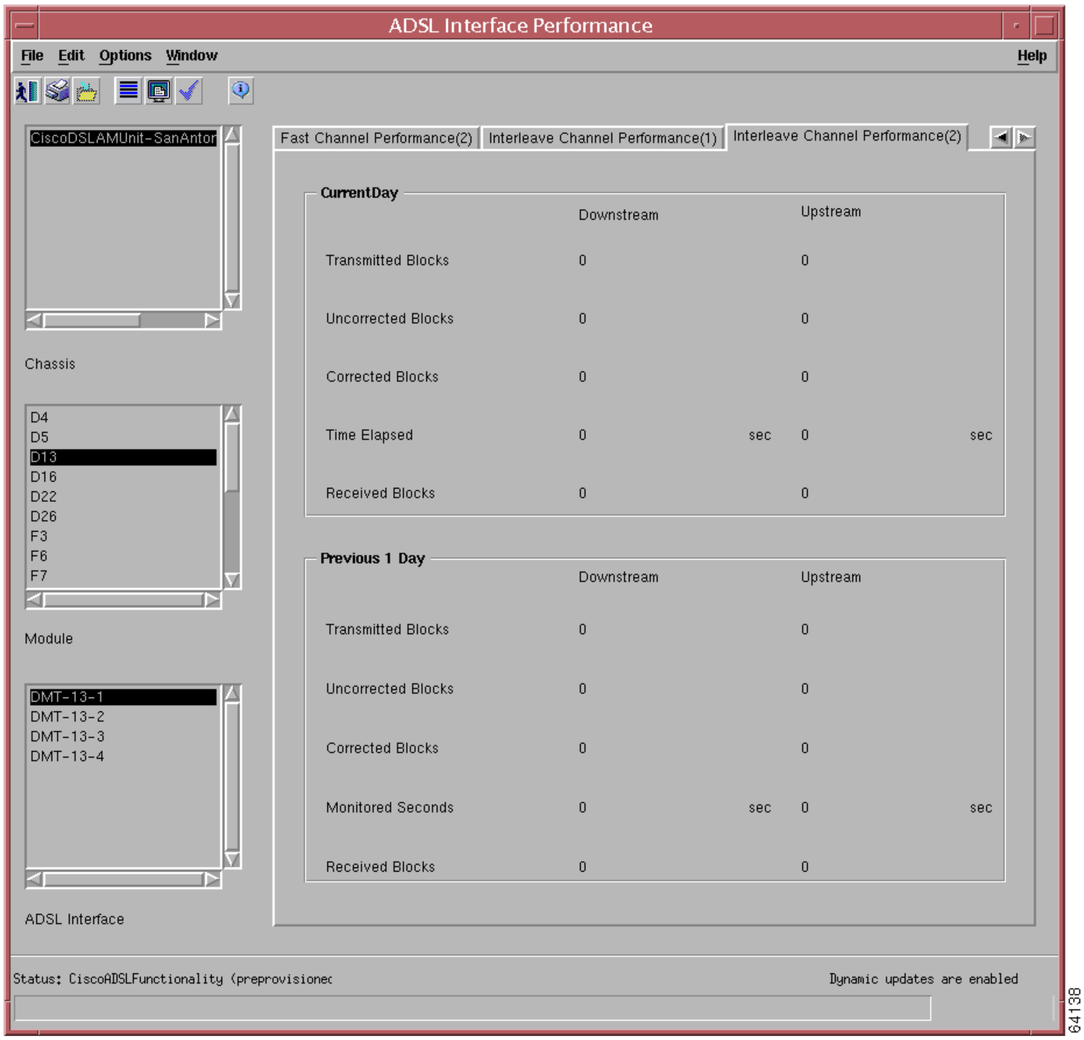
Table 8-8 ADSL Interface Performance Window—Interleave Channel Performance (1) Tab Field Descriptions

Field	Description
Agent Reset	
Transmitted Blocks	Displays the number of blocks of data transmitted since the last agent reset.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted since the last agent reset.
Corrected Blocks	Displays the number of corrected blocks of data transmitted since the last agent reset.
Valid Intervals	Displays the number of intervals since the last agent reset during which data monitoring was valid.
Invalid Intervals	Displays the number of intervals since the last agent reset during which data monitoring was not valid.
Received Blocks	Displays the number of blocks of data received since the last agent reset.
Current 15 Minutes	
Transmitted Blocks	Displays the number of blocks of data transmitted during the current 15-minute interval.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted during the current 15-minute interval.
Corrected Blocks	Displays the number of corrected blocks of data transmitted during the current 15-minute interval.
Time Elapsed	Displays the amount of time that has elapsed since the start of the current 15-minute interval.
Received Blocks	Displays the number of blocks of data received during the current 15-minute interval.

Viewing the ADSL Interface Performance Window—Interleave Channel Performance (2) Tab

The Interleave Channel Performance (2) tab contains two areas—Current Day and Previous 1 Day. (See Figure 8-10.)

Figure 8-10 ADSL Interface Performance Window—Interleave Channel Performance (2) Tab



The ADSL Interface Performance Window Interleave Channel Performance (2) tab fields are described in Table 8-9.

Table 8-9 ADSL Interface Performance Window—Fast Channel Performance (2) Tab Field Descriptions

Field	Description
Current Day	
Transmitted Blocks	Displays the number of blocks of data transmitted during the current day interval.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted during the current day interval.
Corrected Blocks	Displays the number of corrected blocks of data transmitted during the current day interval.
Monitored Seconds	Displays the number of seconds during the current day interval when data was monitored.
Received Blocks	Displays the number of data blocks received during the current day interval.
Previous 1 Day	
Transmitted Blocks	Displays the number of blocks of data transmitted during the previous day interval.
Uncorrected Blocks	Displays the number of uncorrected blocks of data transmitted during the previous day interval.
Corrected Blocks	Displays the number of corrected blocks of data transmitted during the previous day interval.
Monitored Seconds	Displays the number of seconds during the previous day interval when data was monitored.
Received Blocks	Displays the number of data blocks received during the previous day interval.

Viewing SDSL Interface Performance Data

The SDSL Interface Performance window displays performance data for SDSL or G.SHDSL interfaces.

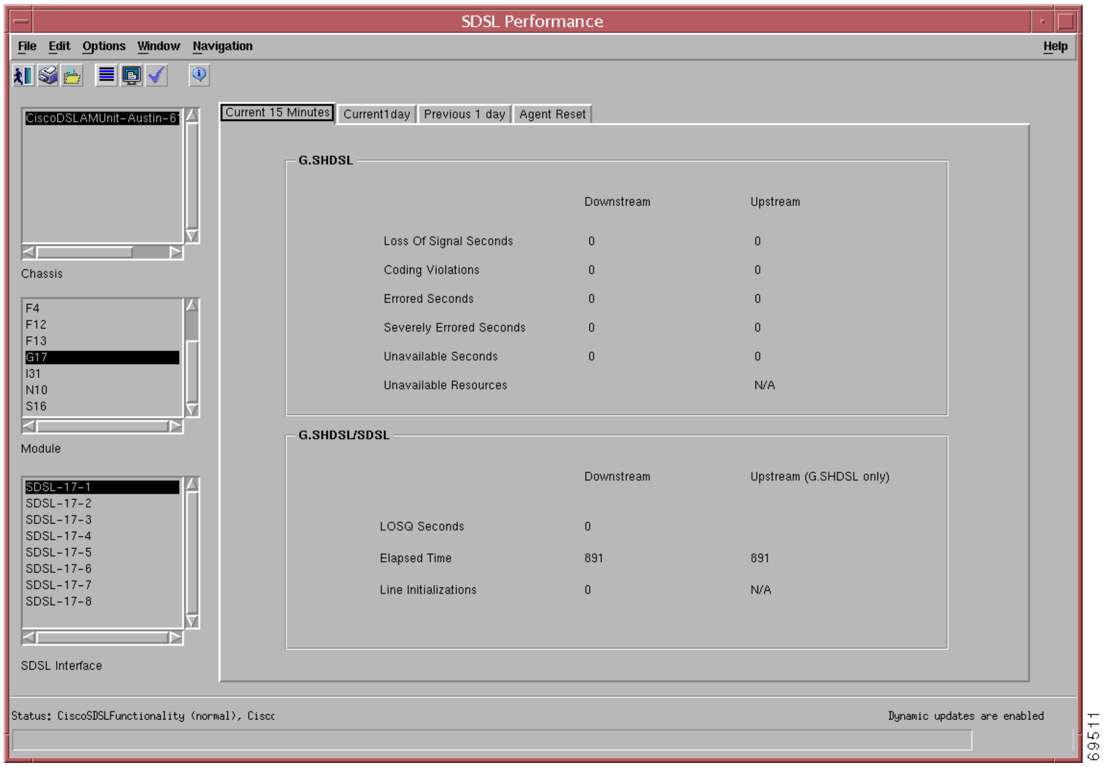
To view the SDSL Performance window, complete the following steps:

Step 1 In the Map Viewer window, within the Physical view, right-click the SDSL or G.SHDSL card whose performance data you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > XDSL > SDSL** from the object menu.

The SDSL Performance window opens. (See Figure 8-11.)

Figure 8-11 SDSL Performance Window



The interface that you selected is highlighted in the list box on the left side of the Map Viewer window. You can also select another SDSL or G.SHDSL interface from the list box.

Step 3 From the list boxes at the left, choose the relevant chassis, card, and SDSL or G.SHDSL interface.

The current performance information for the selected interface displays on the right.

The SDSL Performance window contains four tabs described in the following sections:

- Viewing the SDSL Performance Window Current 15 Minutes Tab, page 8-23
- Viewing the SDSL Performance Window Current 1 Day Tab, page 8-24
- Viewing the SDSL Performance Window Previous 1 Day Tab, page 8-25
- Viewing the SDSL Performance Window Agent Reset Tab, page 8-27

Viewing the SDSL Performance Window Current 15 Minutes Tab

The Current 15 Minutes Tab contains two areas—G.SHDSL and G.SHDSL/SDSL. (See Figure 8-11.)

Table 8-10 describes the fields that are in the Current 15 Minutes tab. Each field contains both a downstream and upstream column, except for the Unavailable Resources and the Line Initializations fields, which display downstream data only.

Table 8-10 SDSL Performance Window—Current 15 Minutes Tab Field Descriptions

Field	Description
G.SHDSL	
Loss of Signal Seconds	Displays the number of seconds since there was loss of signal during the current 15 minutes.
Coding Violations	Displays the number of coding violations encountered by the G.SHDSL interface during the current 15 minutes.
Errored Seconds	Displays the total number of errored seconds encountered by the G.SHDSL interface during the current 15 minutes.
Severely Errored Seconds	Displays the total number of severely errored framing seconds encountered by the G.SHDSL interface during the current 15 minutes.
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the G.SHDSL interface during the current 15 minutes.
Unavailable Resources	Displays the total number of unavailable resources encountered by the G.SHDSL interface during the current 15 minutes.
G.SHDSL/SDSL	
LOSQ[1] Seconds	Displays the number of LOSQ failures experienced by the STU-C for the current 15-minutes. The Upstream column displays G.SHDSL data only.
Elapsed Time	Amount of time that has elapsed. The Upstream column displays G.SHDSL data only.
Line Initializations	Displays the number of line initializations that occurred during the current 15-minute interval.

1. LOSQ = loss of signal quality

Viewing the SDSL Performance Window Current 1 Day Tab

The Current 1 Day Tab contains two areas—G.SHDSL and G.SHDSL/SDSL. (See Figure 8-12.)

Figure 8-12 SDSL Performance Window—Current 1 Day Tab Field Descriptions

Table 8-11 describes the fields that are in the Current 1 Day tab. Each field contains both a downstream and upstream column, except for the Unavailable Resources and the Line Initializations fields, which display downstream data only.

Table 8-11 SDSL Performance Window—Current 1 Day Tab Field Descriptions

Field	Description
G.SHDSL	
Loss of Signal Seconds	Displays the number of seconds since there was loss of signal during the current 1 day.
Coding Violations	Displays the number of coding violations encountered by the G.SHDSL interface during the current 1 day.
Errored Seconds	Displays the total number of errored seconds encountered by the G.SHDSL interface during the current 1 day.
Severely Errored Seconds	Displays the total number of severely errored framing seconds encountered by the G.SHDSL interface during the current 1 day.
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the G.SHDSL interface during the current 1 day.

Table 8-11 SDSL Performance Window—Current 1 Day Tab Field Descriptions (continued)

Field	Description
Unavailable Resources	Displays the total number of unavailable resources encountered by the G.SHDSL interface during the current 1 day.
G.SHDSL/SDSL	
LOSQ Seconds	Displays the number of LOSQ failures experienced by the STU-C for the current 1 day. The Upstream column displays G.SHDSL data only.
Elapsed Time	Amount of time that has elapsed. The Upstream column displays G.SHDSL data only.
Line Initializations	Displays the number of line initializations that occurred during the current 1 day.

Viewing the SDSL Performance Window Previous 1 Day Tab

The Previous 1 Day Tab contains two areas—G.SHDSL and G.SHDSL/SDSL. (See Figure 8-13.)

Figure 8-13 SDSL Performance Window—Previous 1 Day Tab Field Descriptions

Table 8-11 describes the fields that are in the Previous 1 Day tab. Each field contains both a downstream and upstream column, except for the Unavailable Resources and the Line Initializations fields, which display downstream data only.

Table 8-12 SDSL Performance Window—Previous 1 Day Tab Field Descriptions

Field	Description
G.SHDSL	
Loss of Signal Seconds	Displays the number of seconds since there was loss of signal during the previous 1 day.
Coding Violations	Displays the number of coding violations encountered by the G.SHDSL interface during the previous 1 day.
Errored Seconds	Displays the total number of errored seconds encountered by the G.SHDSL interface during the previous 1 day.
Severely Errored Seconds	Displays the total number of severely errored framing seconds encountered by the G.SHDSL interface during the previous 1 day.
Performance Monitoring Seconds	Displays the number of seconds that the interface performance is being monitored in the previous 1 day.
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the G.SHDSL interface during the previous 1 day.
Unavailable Resources	Displays the total number of unavailable resources encountered by the G.SHDSL interface during the previous 1 day.
G.SHDSL/SDSL	
LOSQ Seconds	Displays the number of LOSQ failures experienced by the STU-C for the previous 1 day. The Upstream column displays G.SHDSL data only.
Line Initializations	Displays the number of line initializations that occurred during the previous 1 day.

Viewing the SDSL Performance Window Agent Reset Tab

The Agent Reset Tab contains two areas—G.SHDSL and G.SHDSL/SDSL. (See Figure 8-14.)

Figure 8-14 SDSL Performance Window—Agent Reset Tab Field Descriptions

Table 8-13 describes the fields that are in the Agent Reset tab. Each field contains both a downstream and upstream column, except for the Unavailable Resources and the Line Initializations fields, which display downstream data only.

Table 8-13 SDSL Performance Window—Agent Reset Tab Field Descriptions

Field	Description
G.SHDSL	
Loss of Signal Seconds	Displays the number of seconds since there was loss of signal since agent reset.
Coding Violations	Displays the number of coding violations encountered by the G.SHDSL interface since agent reset.
Errored Seconds	Displays the total number of errored seconds encountered by the G.SHDSL interface since agent reset.
Severely Errored Seconds	Displays the total number of severely errored framing seconds encountered by the G.SHDSL interface since agent reset.
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the G.SHDSL interface since agent reset.

Table 8-13 SDSL Performance Window—Agent Reset Tab Field Descriptions (continued)

Field	Description
Unavailable Resources	Displays the total number of unavailable resources encountered by the G.SHDSL interface since agent reset.
G.SHDSL/SDSL	
LOSQ Seconds	Displays the number of LOSQ failures experienced by the STU-C since agent reset. The Upstream column displays G.SHDSL data only.
Line Initializations	Displays the number of line initializations that occurred since agent reset.
Invalid Performance Intervals	Displays the number of invalid performance intervals since agent reset.
Valid Intervals	Displays the number of valid intervals since agent reset. The Upstream column displays G.SHDSL data only.

Viewing T1/E1 Interface Performance Data

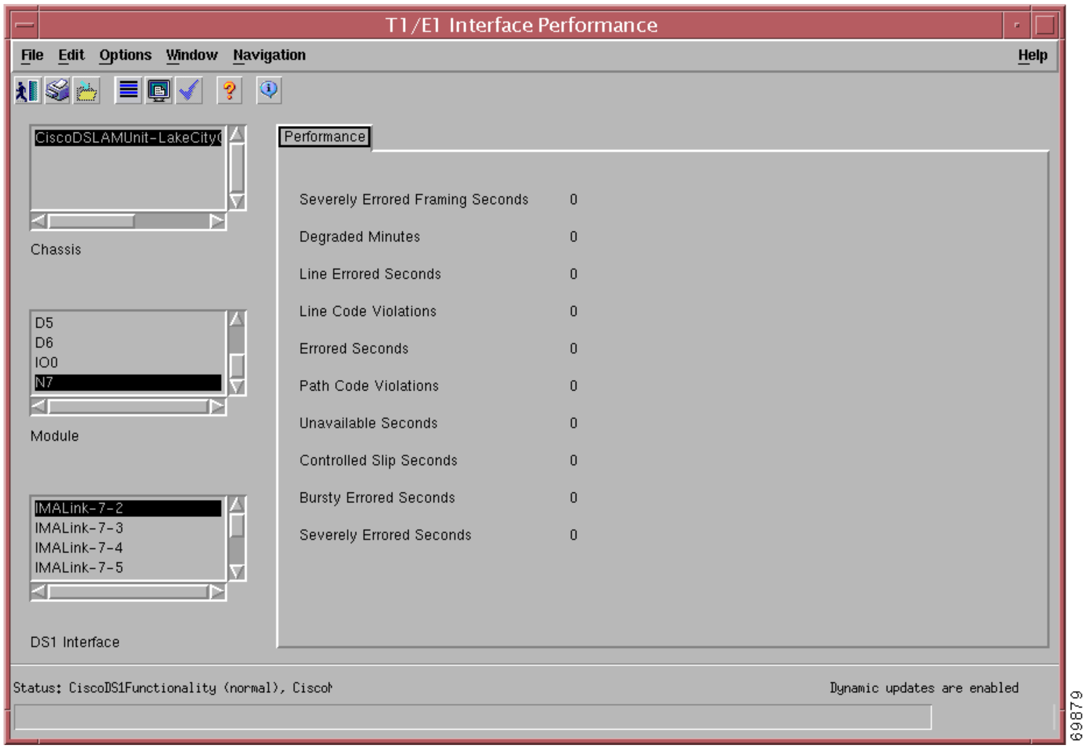
The T1/E1 Interface Performance window displays performance data for the T1/E1 port on the NI-2 card. To view the T1/E1 Interface Performance window, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the NI-2 card for T1/E1 interface whose performance you want to monitor.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > T1/E1** from the object menu.

The T1/E1 Interface Performance window opens. (See Figure 8-16.) The T1/E1 Interface Performance window has one tab—Performance.

Figure 8-15 T1/E1 Interface Performance Window— Performance Tab



The chassis, card, and interface that you selected is highlighted in the list boxes on the left side of the T1/E1 Interface Status window. The current performance information for the selected T1/E1 interface appears on the right.

The fields in T1/E1 Interface Status window are described in Table 8-15.

Table 8-14 T1/E1 Interface Performance Window Field Descriptions

Field	Description
Severely Errored Framing Seconds	Displays the number of severely errored framing seconds that the DS1 interface encountered in the current 15-minute interval.
Degraded Minutes	Displays the number of degraded minutes that the DS1 interface encountered in the current 15-minute interval.
Line Errored Seconds	Displays the number of line errored seconds that the DS1 interface encountered in the current 15-minute interval.
Line Code Violations	Displays the number of line code violations that the DS1 interface encountered in the current 15-minute interval.
Errored Seconds	Displays the number of errored seconds that the DS1 interface encountered in the current 15-minute interval.

Table 8-14 T1/E1 Interface Performance Window Field Descriptions (continued)

Field	Description
Path Code Violations	Displays the number of path code violations that the DS1 interface encountered in the current 15-minute interval.
Unavailable Seconds	Displays the number of unavailable seconds that the DS1 interface encountered in the current 15-minute interval.
Controlled Slip Seconds	Displays the number of controlled slip seconds that the DS1 interface encountered in the current 15-minute interval.
Bursty Errored Seconds	Displays the number of bursty errored seconds that the DS1 interface encountered in the current 15-minute interval.
Severely Errored Seconds	Displays the number of severely errored seconds that the DS1 interface encountered in the current 15-minute interval.

Viewing DS3/E3 Interface Performance Data

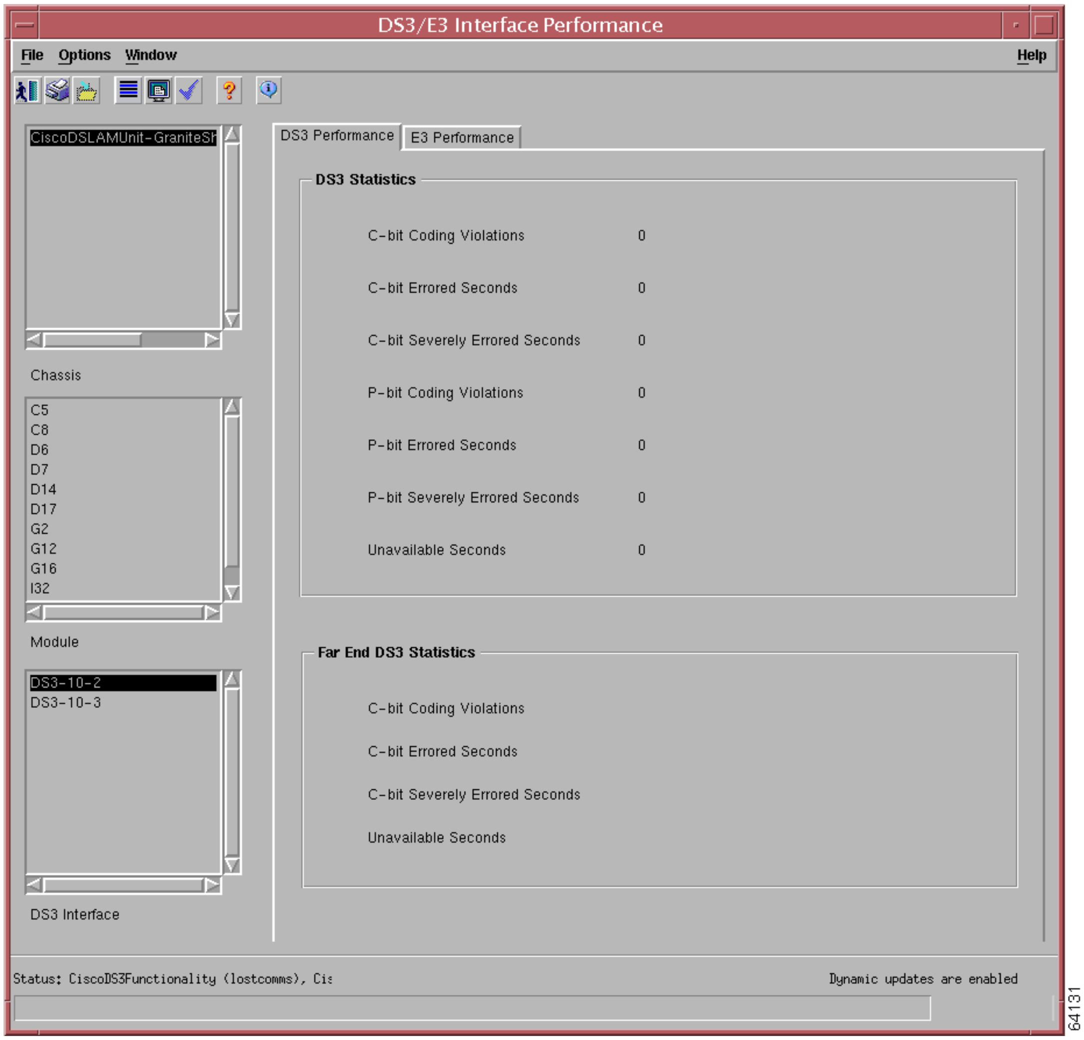
The DS3/E3 Interface Performance window displays performance data for the DS3/E3 port on the NI-2 card. To view the DS3/E3 Interface Performance window, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the NI-2 card for DS3/E3 interface whose performance you want to monitor.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > DS3/E3** from the object menu.

The DS3/E3 Interface Performance window opens. (See Figure 8-16.) The DS3/E3 Interface Performance window has two tabs—DS3 Performance and E3 Performance.

Figure 8-16 DS3 Interface Performance Window—DS3 Performance Tab



The chassis, card, and interface that you selected is highlighted in the list boxes on the left side of the DS3/E3 Interface Status window. The current performance information for the selected DS3/E3 interface appears on the right.

The DS3 Performance tab contains two areas, DS3 Statistics, and Far End DS3 Statistics. The fields in this tab are described in Table 8-15.

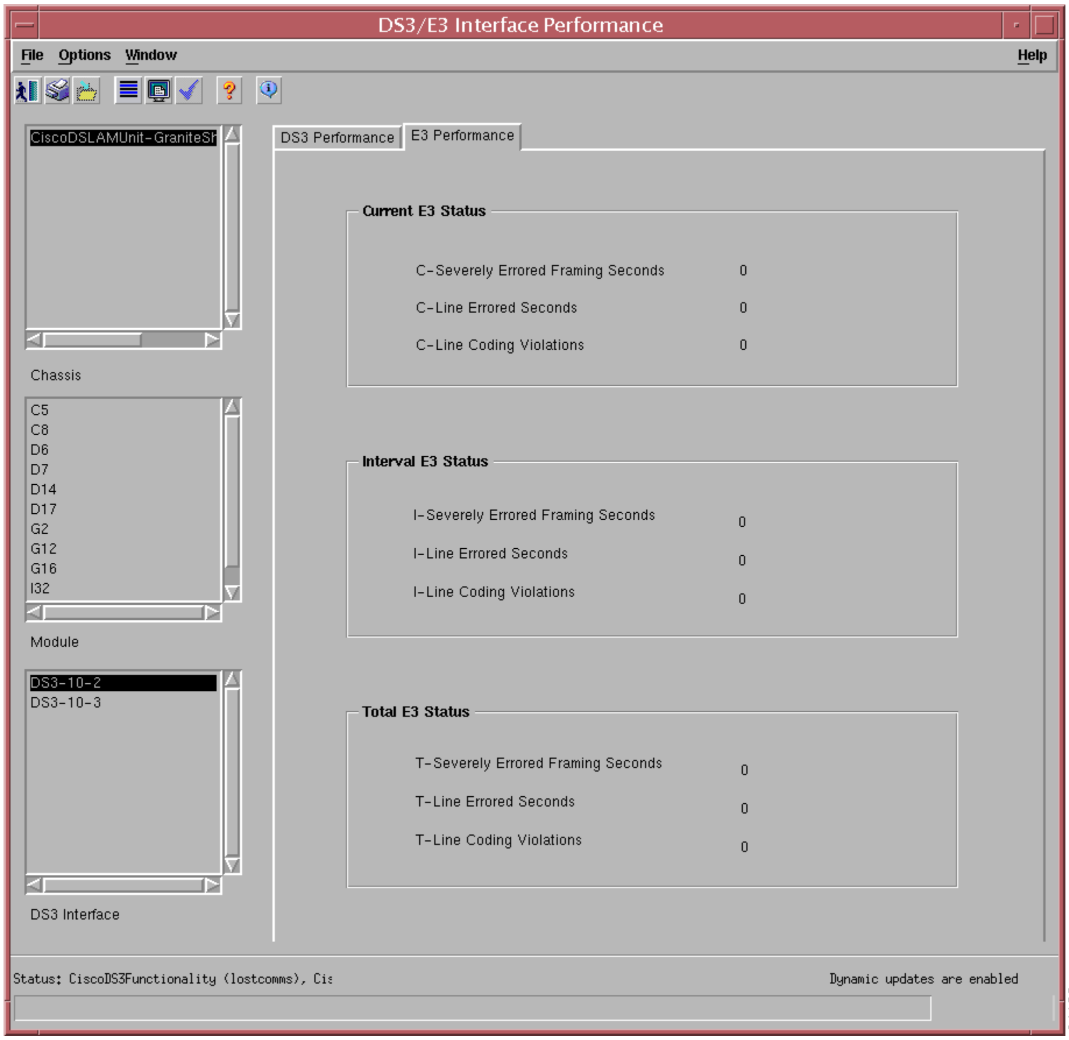
Table 8-15 DS3/E3 Interface Performance Window—DS3 Performance Tab Field Descriptions

Field	Description
DS3 Statistics	
C-bit[1] Coding Violations	Counts the number of C-bit coding violations that a DS3 interface encountered in the current 15-minute interval.
C-bit Errored Seconds	Counts the number of C-bit errored seconds that a DS3 interface encountered in the current 15-minute interval.
C-bit Severely Errored Seconds	Counts the number of C-bit severely errored seconds that a DS3 interface encountered in the current 15-minute interval.
P-bit Coding Violations	Counts the number of P-bit coding violations that a DS3 interface encountered in the current 15-minute interval.
P-bit Errored Seconds	Counts the number of P-bit errored seconds that a DS3 interface encountered in the current 15-minute interval.
P-bit Severely Errored Seconds	Counts the number of P-bit severely errored seconds that a DS3 interface encountered in the current 15-minute interval.
Unavailable Seconds	Counts the number of P-bit unavailable seconds that a DS3 interface encountered in the current 15-minute interval.
Far End DS3 Statistics	
C-bit Coding Violations	Counts the number of far-end, C-bit coding violations that a DS3 interface encountered in the current 15-minute interval.
C-bit Errored Seconds	Counts the number of far-end, C-bit errored seconds that a DS3 interface encountered in the current 15-minute interval.
C-bit Severely Errored Seconds	Counts the number of far-end, C-bit severely errored seconds that a DS3 interface encountered in the current 15-minute interval.
Unavailable Seconds	Counts the number of far-end, C-bit unavailable seconds that a DS3 interface encountered in the current 15-minute interval.

1. C-bit = Signaling and control bits used in some T-carrier systems for synchronization and parity-checking error control.

The DS3/E3 Interface Performance window E3 Performance tab is shown in Figure 8-17.

Figure 8-17 DS3/E3 Interface Performance Window—E3 Performance Tab



The DS3/E3 Interface Performance window E3 Performance tab contains three areas—Current E3 Status, Interval E3 STatus, and Total E3 Status. The fields in this tab are described in Table 8-16.

Table 8-16 DS3/E3 Interface Performance Window—E3 Performance Tab Field Descriptions

Field	Description
Current E3 Status	
C-Severely Errored Framing Seconds	Counts the number of current, severely errored framing seconds that an E3 interface encountered in the current 15-minute interval.
C-Line Errored Seconds	Counts the number of current, line errored seconds that an E3 interface encountered in the current 15-minute interval.
C-Line Coding Violations	Counts the number of current, line coding violations that an E3 interface encountered in the current 15-minute interval.

Table 8-16 DS3/E3 Interface Performance Window—E3 Performance Tab Field Descriptions

Field	Description
Interval E3 Status	
I-Severely Errored Framing Seconds	Counts the number of severely errored framing seconds that an E3 interface encountered in one of the previous 96 individual 15-minute intervals.
I-Line Errored Seconds	Counts the number of errored framing seconds that an E3 interface encountered in one of the previous 96 individual 15-minute intervals.
I-Line Coding Violations	Counts the number of coding violations that an E3 interface encountered in one of the previous 96 individual 15-minute intervals.
Total E3 Status	
T-Severely Errored Framing Seconds	Counts the total number of severely errored framing seconds that an E3 interface encountered in the previous 24-hour interval.
T-Line Errored Seconds	Counts the total number of line errored seconds that an E3 interface encountered in the previous 24-hour interval.
T-Line Coding Violations	Counts the total number of line coding violations that an E3 interface encountered in the previous 24-hour interval.

Viewing ATM Interface Performance Data

This section includes the following topics:

- Viewing the ATM Interface Performance Window Transmitted and Received Areas, page 8-36
- Viewing the ATM Interface Performance Connection Established Area, page 8-39

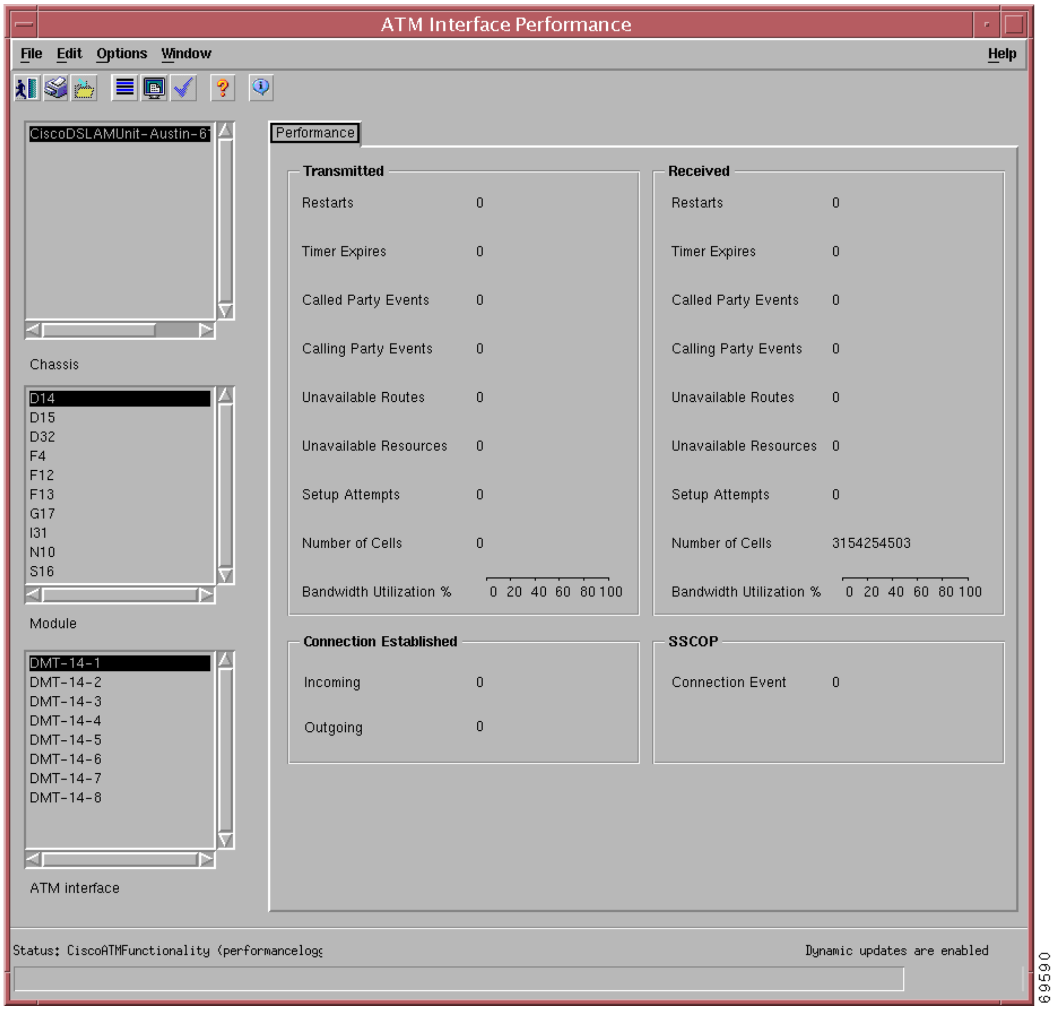
To view the ATM Interface Performance data window, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click either the DMT line card or a NI-2 card whose performance data you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > ATM** from the object menu.

The ATM Interface Performance window opens. (See Figure 8-18.) The ATM Interface Performance window has one tab, the Performance tab.

Figure 8-18 ATM Interface Performance Window



> **Note** CDM automatically creates four DMT interfaces when you deploy a DMT line card. These DMT interfaces are actually ATM over ADSL over DMT interfaces. This means that all three interfaces are combined in CDM and identified by the last specific DMT interface. Therefore, when you view performance information for an ATM interface, it is identified as a DMT interface.

The relevant chassis, card, and ATM interface that you selected is highlighted in the list boxes on the left side of the window. The current performance information for the selected ATM interface displays on the right.

The Performance tab contains four areas:

- Transmitted
- Received
- Connection Established
- Service Specific Connection-Oriented Protocol (SSCOP)

These tabs are described in the following sections.

Viewing the ATM Interface Performance Window Transmitted and Received Areas

Received and transmitted gauges are displayed from a subscriber point of view. The transmitted values display the number of cells per second that the subscriber is transmitting. The received values display the number of cells per second that the subscriber is receiving.

The Transmitted and Received areas display the same attribute parameters, which are described in Table 8-17.

Table 8-17 ATM Interface Performance Window Field Descriptions

Field	Description
Transmitted and Received	
Restarts	Displays the number of Restart Activity errors that are transmitted from or received by this interface. The Restart Activity Counter provides a count of host, switch, or network restart activity. This counter is incremented when transmitting or receiving a Restart message.
Timer Expires	Displays the number of Timer Expires transmitted from or received by this interface. The Timer Expires counter provides a count of network timer expiries, and to some extent, host or switch timer expiries. The Timer Expires counter is incremented whenever one of the following conditions occurs: • Expiration of any network timer • Receipt of a Release or Release Complete message • Recovery on timer expiration

Table 8-17 ATM Interface Performance Window Field Descriptions (continued)

Field	Description
Called Party Events	Displays the number of Called Party Events messages transmitted from or received by this interface. This counter is incremented when a Release, Release Complete (only when not preceded by a Release message for the same call), Add Party Reject, or Status message is transmitted or received that contains one of the following cause code values: • 17—User busy • 18—No user responding • 21—All rejected • 22—Displays the number changed • 23—User rejects all calls with calling line ID restriction (CLIR) • 27—Destination out of order • 31—Normal, unspecified • 88—Incompatible destination **Note** A cause code value alerts you that something is wrong with your ISDN connection. A cause code value applies to both User Network Interface (UNI) Version 3.0 and UNI Version 3.1. A UNI is an interface point between ATM end users and a private ATM switch, or between a private ATM switch and the public carrier ATM network.
Calling Party Events	Displays the number of Calling Party Events messages transmitted from or received by this interface. This counter reflects error events that occur due to the originating user performing an incorrect action. This counter is incremented when a Release, Release Complete (only when not preceded by a Release message for the same call), Add Party Reject, or Status message is transmitted or received that contains one of the following cause code values: • 28—Invalid number format (address incomplete) • 43—Access information discarded • 57—Bearer capability not authorized • 65—Bearer capability not implemented • 73—Unsupported combination of traffic parameters • 78—AAL parameters cannot be supported (UNI 3.1 only) • 91—Invalid transit network selection • 93—AAL parameters cannot be supported (UNI 3.0 only) **Note** These cause code values apply to both UNI 3.0 and UNI 3.1.

Table 8-17 ATM Interface Performance Window Field Descriptions (continued)

Field	Description
Unavailable Routes	Displays the number of Route Unavailability messages transmitted from or received by this interface. This counter is incremented when a Release, Release Complete (only when not preceded by a Release message for the same call), Add Party Reject, or Status message is transmitted or received that contains one of the following cause code values: • 1—Unallocated (unassigned) number • 2—No route to specified transit network • 3—No route to destination **Note** For this counter, Release Complete messages that are a reply to a previous Release message and contain the same cause code value, are redundant (for counting purposes) and should not be counted. These cause code values apply to both UNI 3.0 and UNI 3.1.
Unavailable Resources	Displays the number of Resource Unavailability messages transmitted from or received by this interface. This counter is incremented when a Release, Release Complete (only when not preceded by a Release message for the same call), Add Party Reject, or Status message is transmitted or received that contains one of the following cause code values. • 35—Requested VPCI / VCI not available • 37—User cell rate not available (UNI 3.1 only) • 38—Network out of order • 41—Temporary failure • 45—No VPCI / VCI available • 47—Resource unavailable, unspecified • 49—Quality of Service unavailable • 51—User cell rate not available (UNI 3.0 only) • 58—Bearer capability not presently available • 63—Service or option not available, unspecified • 92—Too many pending add party requests **Note** These cause code values apply to both UNI 3.0 and UNI 3.1.
Setup Attempts	Displays the number of call setup attempts (both successful and unsuccessful) transmitted from or received by this interface.
Number of Cells	Displays the number of cells transmitted from or received by this interface, including p2p and p2mp cells.
Bandwidth Utilization	Displays the used bandwidth as a percentage of the maximum bandwidth supported by the port.

Viewing the ATM Interface Performance Connection Established Area

The Connection Established area displays the fields that are described in Table 8-18.

Table 8-18 Connection Established Field Descriptions

Field	Description
Connection Established	
Incoming	Displays the number of switched virtual connections (SVCs) virtual channel connections (VCCs) established at the signaling entity for incoming connections.
Outgoing	Displays the number of SVC VCCs established at the signaling entity for outgoing connections.
SSCOP[1]	
Connection Event	Displays the number of connection events on this interface: • SSCOP Connection Disconnect Counter—The abnormal occurrence of the event is characterized by the expiration of Timer_NO_RESPONSE. (The event is communicated to the layer management with MAA-ERROR code P. Refer to ITU-T Q.2110 [13].) • SSCOP Connection Initiation Failure—The condition indicates the inability to establish an SSCOP connection. The event occurs whenever the number of expires of the connection control timer (Timer_CC) exceeds the MaxCC value or whenever a connection reject message BGREJ PDU is received. (The event is communicated to layer management with MAA-ERROR code O. Refer to ITU-T Q.2110.) • SSCOP Connection Re-establ/Resynch—Occurs upon receipt of a BGN PDU or RESYNC PDU.

1. SSCOP = Service-Specific Connection-Oriented Protocol

Viewing IMA Group and Link Performance

The inverse multiplexing over ATM (IMA) Group Performance and Link Performance windows display information about the IMA connections. These windows are described in the following sections:

- Viewing IMA Group Performance Data, page 8-39
- Viewing IMA Link Performance Data, page 8-41

Viewing IMA Group Performance Data

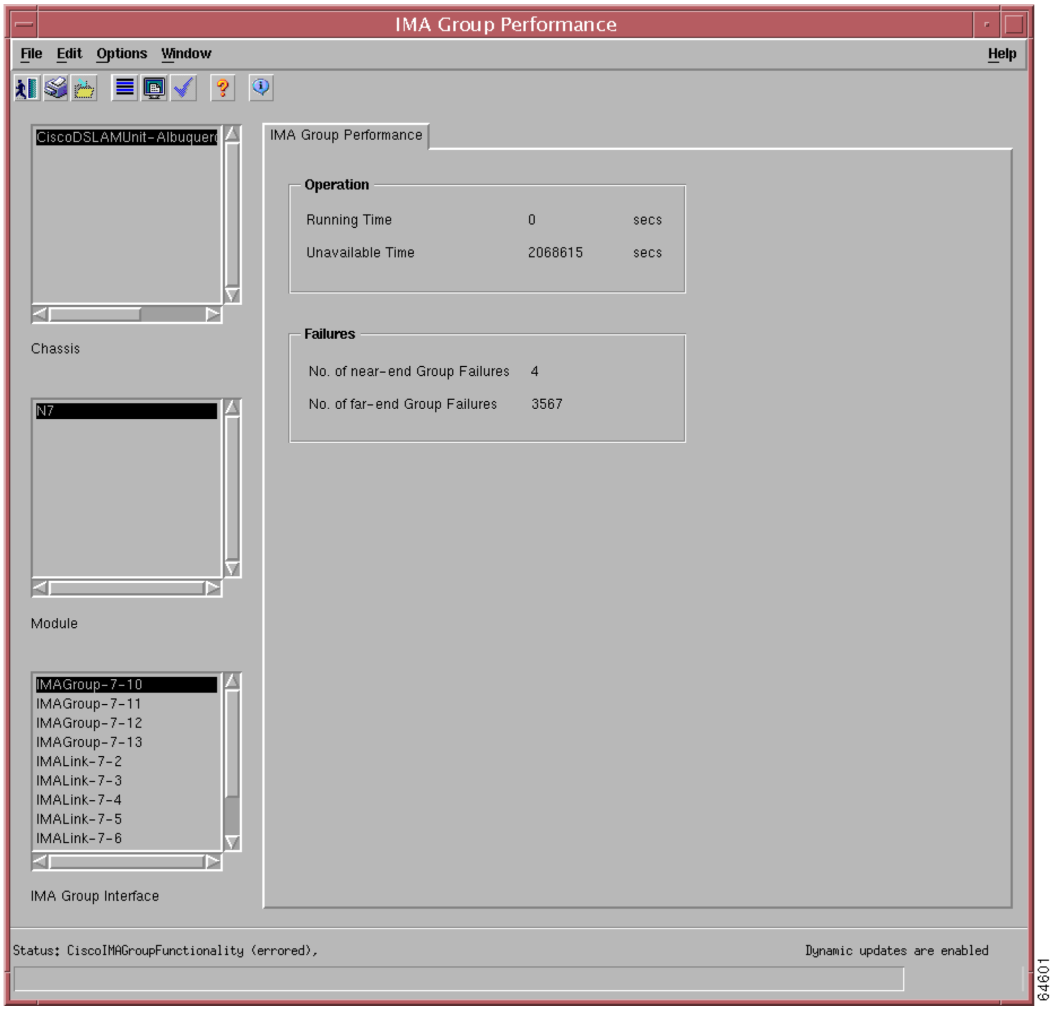
To open the IMA Group Performance window, complete the following steps:

Step 1 From the left side of the Map Viewer window, from within the Physical hierarchy view, right-click the IMA group whose performance statistics you want to monitor.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > IMA Group** from the object menu.

The IMA Group Performance window opens. (See Figure 8-19.)

Figure 8-19 IMA Group Performance Window



This window contains two areas—Operation and Failures. The fields in this window are described in Table 8-19.

Table 8-19 IMA Group Performance Window Field Descriptions

Field	Description
Operation	
Running Time	Displays a count of the IMA group running seconds.
Unavailable Time	Displays a count of the IMA group unavailable seconds.

Table 8-19 IMA Group Performance Window Field Descriptions

Field	Description
Failures	
No. of near-end Group Failures	Displays the number of times that a near-end group failure (Config-Abort, Insufficient-Links) has been reported since power up or reboot.
No. of far-end Group Failures	Displays the number of times that a far-end group failure (Config-Abort-FE, Insufficient-Links-FE, Blocked-FE) has been reported since power up or reboot. This is an optional attribute.

Viewing IMA Link Performance Data

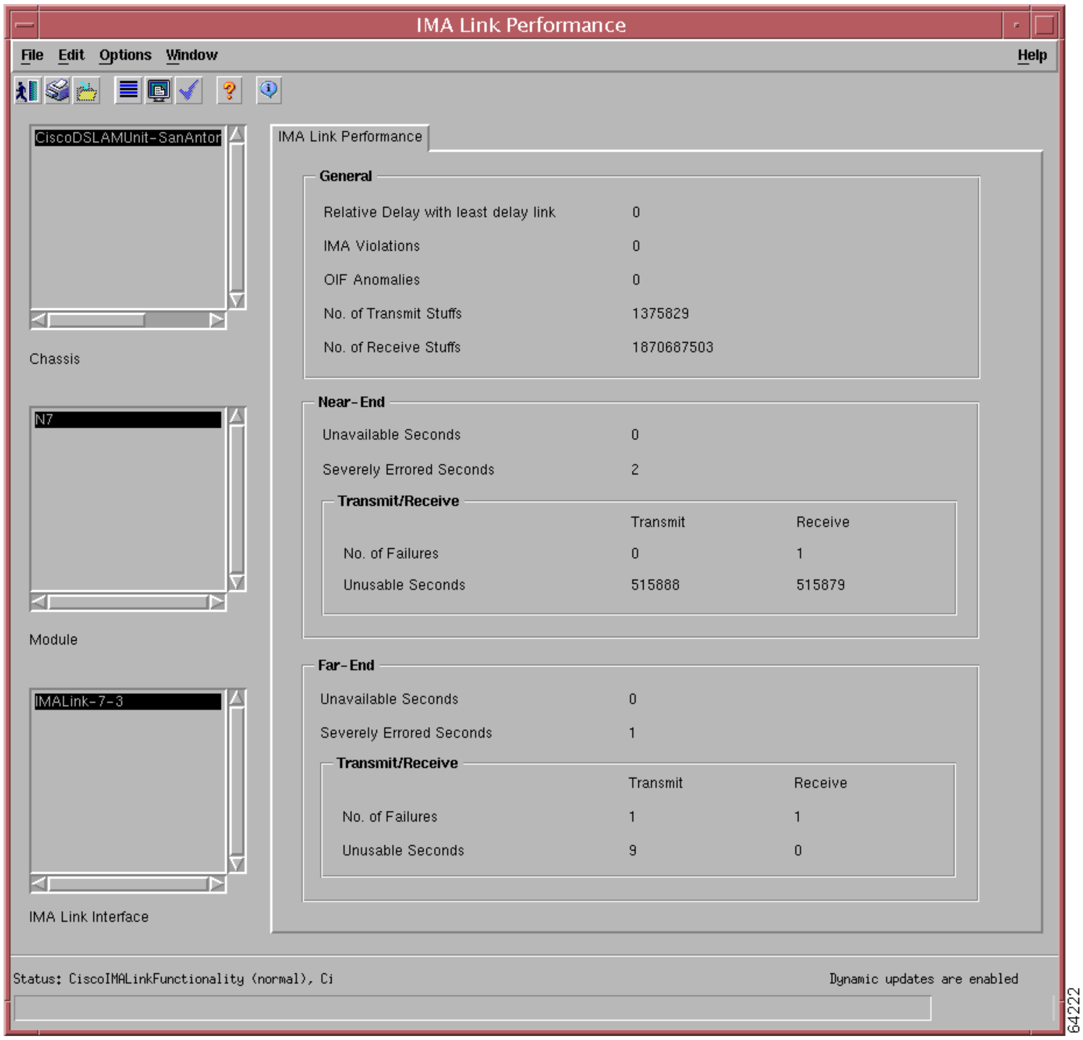
To open the IMA Link Performance window, complete the following steps:

Step 1 From the left side of the Map Viewer window, from within the IMA hierarchy view, right-click the IMA link whose performance data you want to monitor.

Step 2 Choose **Cisco DSL Manager > Interface > Performance > IMA Link** from the object menu.

The IMA Link Performance window opens. (See Figure 8-20.)

Figure 8-20   IMA Link Performance Window



This window includes the following areas:

- General
- Near-End—Transmit/Receive
- Far-End—Transmit/Receive

The fields in this window are described in Table 8-20.

Table 8-20 IMA Link Performance Window Field Descriptions

Field	Description
General	
Relative Delay with least delay link	Displays the latest measured delay on this link relative to the link, in the same IMA group, with the least delay.
IMA Violations	Displays a count of errored, invalid, or missing ICP[1] cells, except during SES[2]-IMA or UAS[3]-IMA conditions.
OIF Anomalies	Displays the number of OIF anomalies, except during SES-IMA or UAS-IMA conditions, at the near-end. This is an optional attribute.
No. of Transmit Stuffs	Displays a count of stuff events that are inserted in the transmit direction in the current 15-minute interval. This is an optional attribute.
No. of Receive Stuffs	Displays a count of stuff events that are inserted in the receive direction in the current 15-minute interval. This is an optional attribute.
Near End	
Unavailable Seconds	Displays a count of unavailable seconds at the near end in one of the previous 96 individual 15-minute intervals. Unavailability begins at the onset of 10 contiguous SES-IMA and ends at the onset of 10 contiguous seconds with no SES-IMA.
Severely Errored Seconds	Displays a count of 1-second intervals that contain one of the following items except during a UAS-IMA condition, in the previous 24 hour interval: • >= 30% of the ICP that are cells counted as IV-IMAs • One or more link defects (that is, LOS[4], OOF/LOF[5], AIS[6], or LCD[7]) • LIF defects • LODS defects Invalid 15-minute intervals count as 0.
No. of Failures	Displays the number of transmit failures and receive failures at the near end.
Unusable seconds	Displays a count of unusable seconds at the near end.
Far End	
Unavailable Seconds	Displays a count of unavailable seconds at the far end in one of the previous 96, individual 15-minute interval. Unavailability begins at the onset of 10 contiguous SES-IMA-FE and ends at the onset of 10 contiguous seconds with no SES-IMA-FE.

Table 8-20 IMA Link Performance Window Field Descriptions (continued)

Field	Description
Severely Errored Seconds	Displays a count of 1-second intervals that contain one or more RDI[8]-IMA defects, except during a UAS-IMA-FE condition, in the previous 24 hour interval. Invalid 15-minute intervals count as 0.
No. of Failures	Displays the number of transmit failures and receive failures at the far end.
Unusable seconds	Displays a count of unusable seconds at the far end.

1. ICP = intelligent call processing
2. SES = severely errored second
3. UAS = unavailable seconds
4. LOS = loss of signal
5. OOF/LOF = out of frame/loss of frame
6. AIS = alarm indication signal
7. LCD = logical channel device
8. RMI = remote detect indication

Viewing SONET (OC3) Interface Performance Data

This section includes the following topics:

- Viewing the SONET Interface Performance Window—Section Tab, page 8-46
- Viewing the SONET Interface Performance Window—Line Tab, page 8-47
- Viewing the SONET Interface Performance Window—Path Tab, page 8-49

The SONET Interface Performance window displays performance data for the SONET interfaces.

Note SONET and OC-3 interfaces are the same thing.

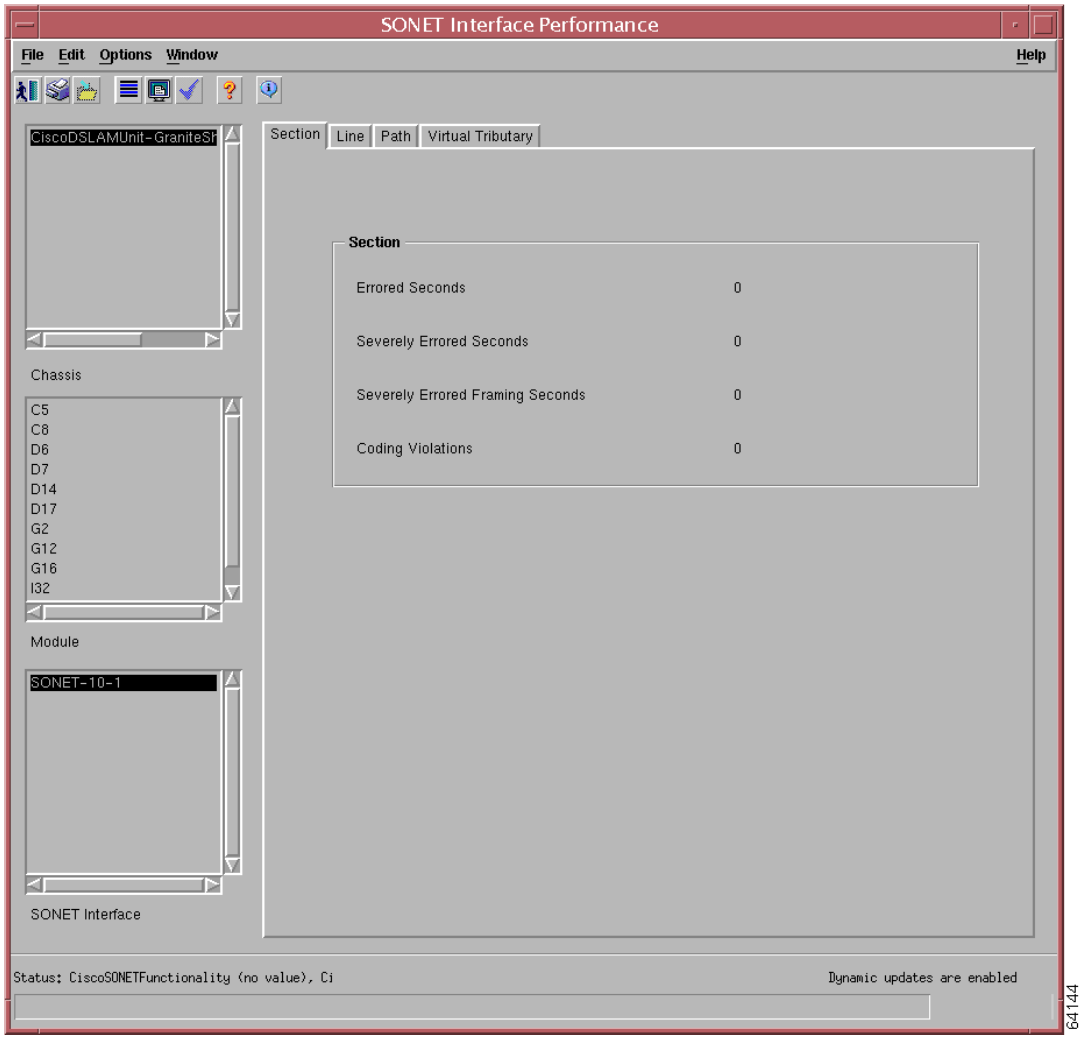
To view the SONET Interface Performance window, follow these steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the NI-2 card whose performance data you want to view.

Step 2 Choose **Cisco DSL Manager > Interface > Performance SONET** from the object menu.

The SONET Interface Performance window opens. (See Figure 8-21.)

Figure 8-21 SONET Interface Performance Window



Step 3 From the list boxes on the left, select the relevant chassis, card, and SONET interface.

The relevant chassis, card, and SONET interface that you selected are highlighted in the list boxes on the left side of the window. The current performance information for the selected SONET interface displays on the right.

The SONET Interface Performance window contains four tabs:

- Section
- Line
- Path
- Virtual Tributary—not used in CDM

The fields in these tabs are described in the following sections.

Viewing the SONET Interface Performance Window—Section Tab

The Section tab window contains one area, Section (see Figure 8-21). The fields in this tab are described in Table 8-21.

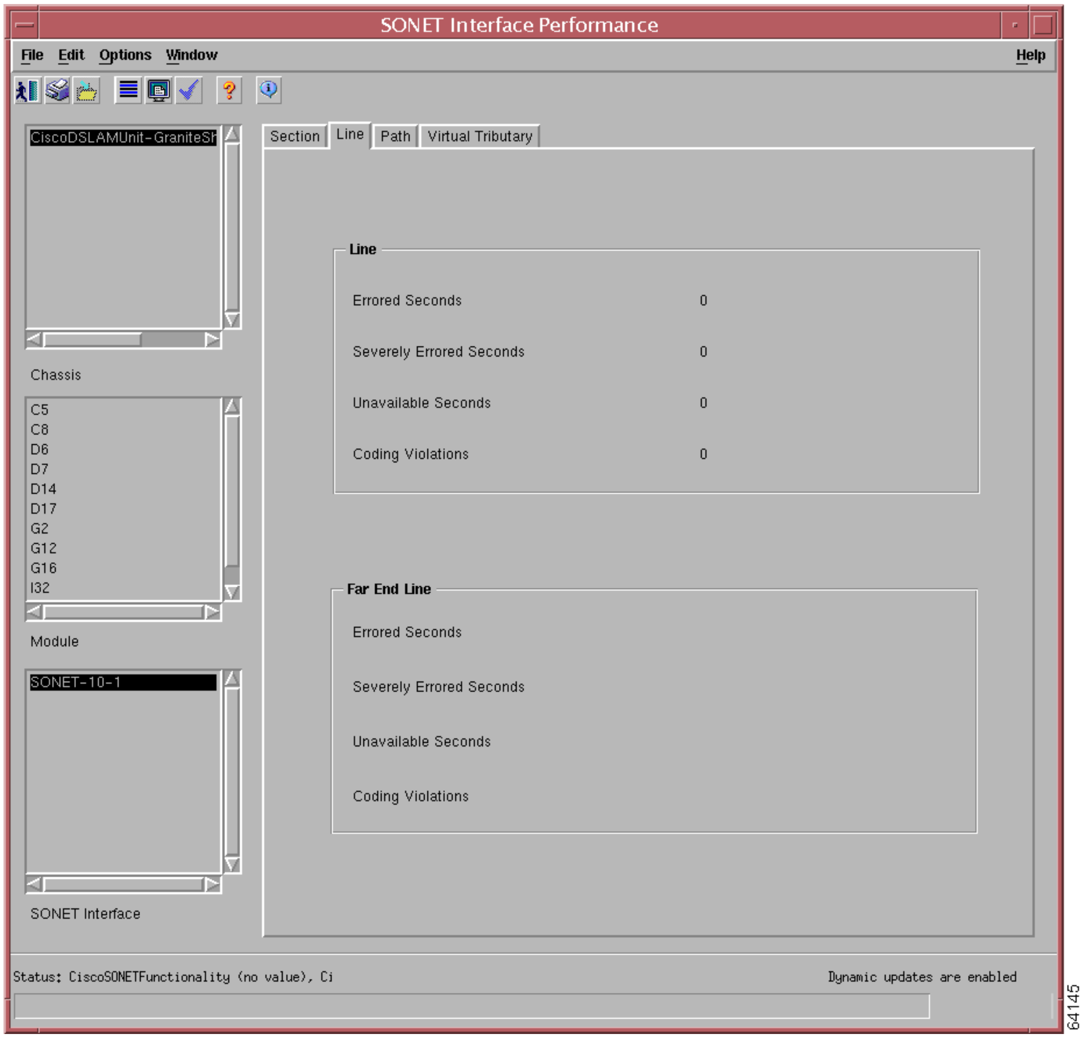
Table 8-21 SONET Interface Performance Window—Section Tab Field Descriptions

Field	Description
Errored Seconds	Displays the total number of errored seconds encountered by the SONET interface.
Severely Errored Seconds	Displays the number of severely errored seconds encountered by the SONET interface.
Severely Errored Framing Seconds	Displays the total number of severely errored framing seconds encountered by the SONET interface.
Coding Violations	Displays the number of coding violations encountered by the SONET interface.

Viewing the SONET Interface Performance Window—Line Tab

The Line tab contains two areas—Line and Far End Line. (See Figure 8-22.)

Figure 8-22 SONET Interface Performance Window—Line Tab



The fields in this tab are described in Table 8-22. The Line and Far End Line areas contain the same fields.

Table 8-22 SONET Interface Performance Window—Line Tab Field Descriptions

Field	Description
Line	
Errored Seconds	Displays the total number of errored seconds encountered by the SONET interface.
Severely Errored Seconds	Displays the number of severely errored seconds encountered by the SONET interface.

Table 8-22 SONET Interface Performance Window—Line Tab Field Descriptions (continued)

Field	Description
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the SONET interface.
Coding Violations	Displays the number of coding violations encountered by the SONET interface.
Far End Line	
Errored Seconds	Displays the total number of errored seconds encountered by the SONET interface.
Severely Errored Seconds	Displays the number of severely errored seconds encountered by the SONET interface.
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the SONET interface.
Coding Violations	Displays the number of coding violations encountered by the SONET interface.

Viewing the SONET Interface Performance Window—Path Tab

The Path tab contains two areas—Path and Far End Path. (See Figure 8-23.)

Figure 8-23 SONET Interface Performance Window—Path Tab

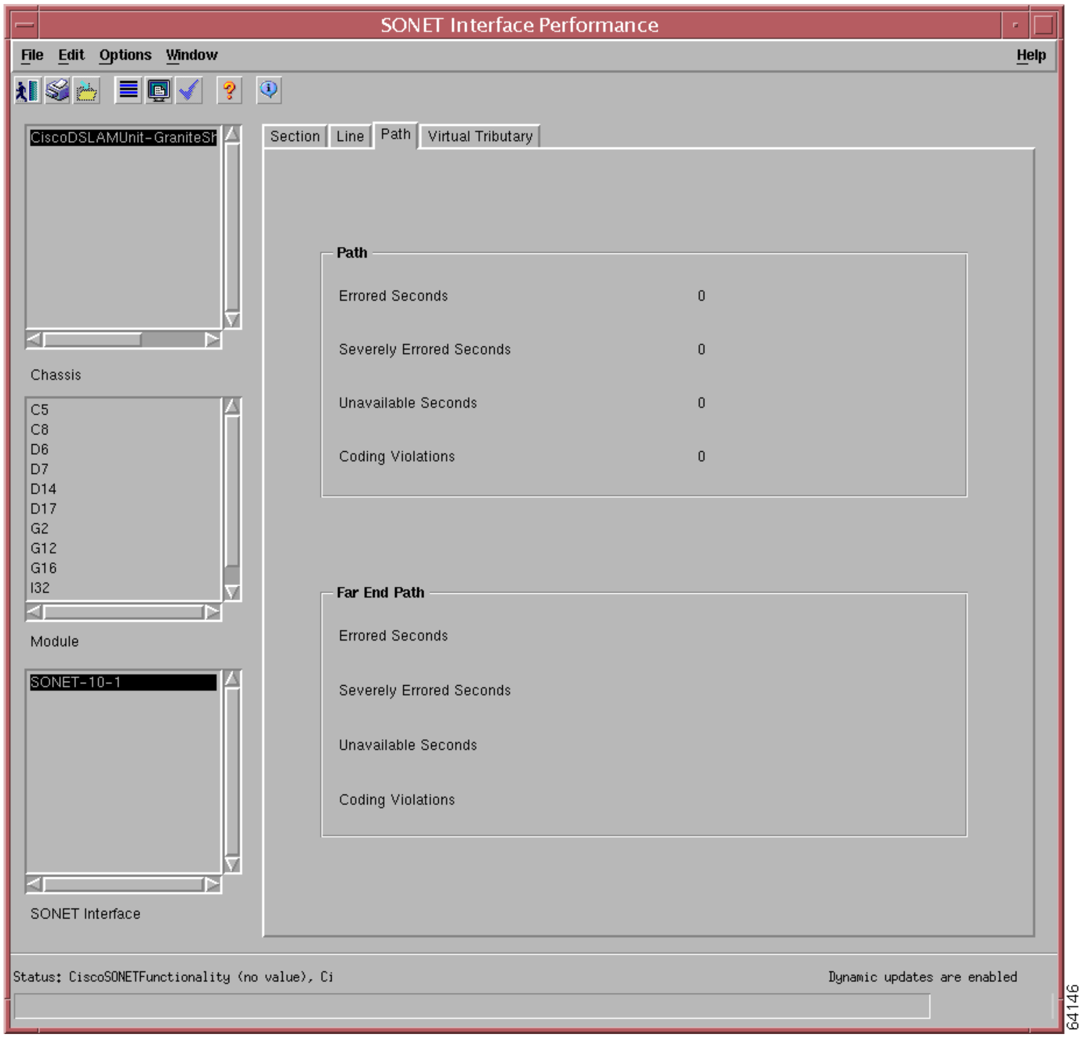


Table 8-21 describes the fields that are in the Path tab. The Path and Far End Path areas contain the same fields.

Table 8-23 SONET Interface Performance Window—Path Tab Field Descriptions

Field	Description
Path	
Errored Seconds	Displays the total number of errored seconds encountered by the SONET interface.
Severely Errored Seconds	Displays the number of severely errored seconds encountered by the SONET interface.

Table 8-23 SONET Interface Performance Window—Path Tab Field Descriptions (continued)

Field	Description
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the SONET interface.
Coding Violations	Displays the number of coding violations encountered by the SONET interface.
Far End Path	
Errored Seconds	Displays the total number of errored seconds encountered by the SONET interface.
Severely Errored Seconds	Displays the number of severely errored seconds encountered by the SONET interface.
Unavailable Seconds	Displays the total number of unavailable seconds encountered by the SONET interface.
Coding Violations	Displays the number of coding violations encountered by the SONET interface.

Viewing Historical Performance Data

This section describes how to use the Performance Manager window to view historical data as well as current data in the form of a line chart, bar chart, or table. This section also describes how to view DS3/E3 or OC-3 interface performance data and how to view ATM over ADSL over DMT interface performance data.

This section includes the following topics:

- Setting the Chassis to Performance Logging On State, page 8-50
- Viewing DS3/E3 or OC-3 Interface Performance Data, page 8-51
- Viewing ATM over ADSL over DMT Interface Performance Data, page 8-56

Setting the Chassis to Performance Logging On State

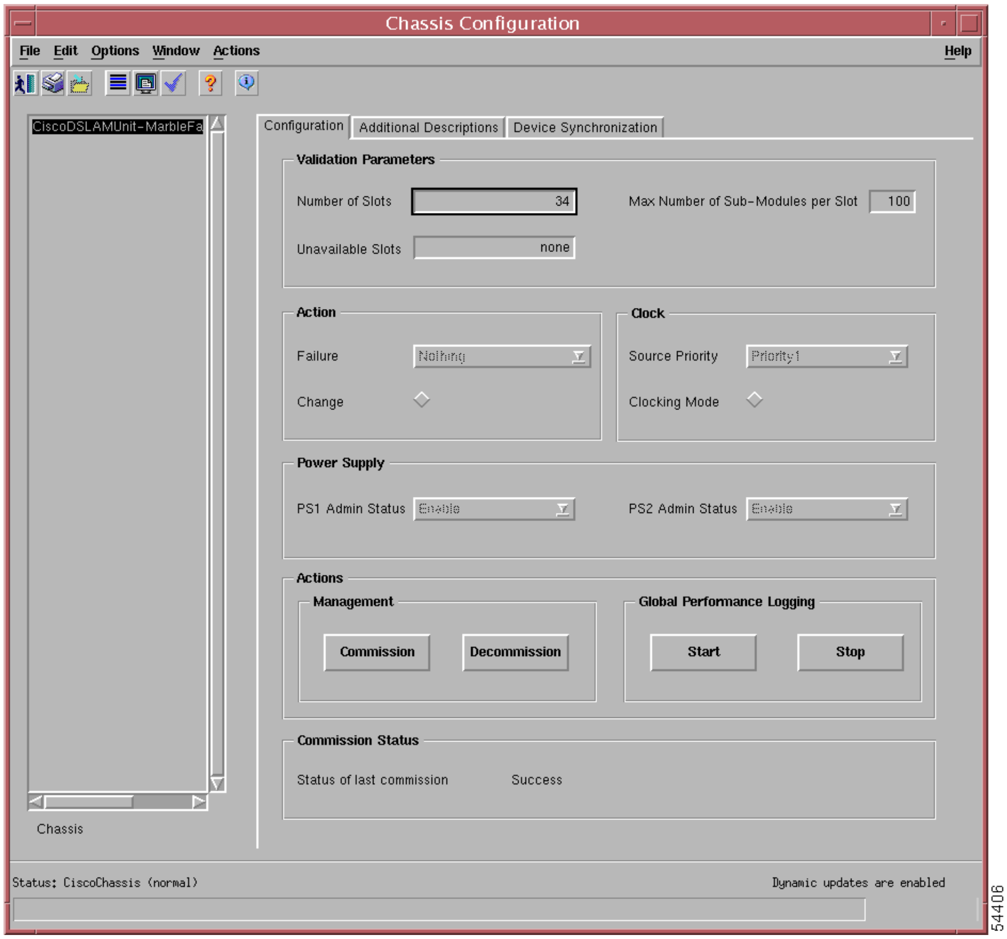
Before you can view historical performance data, you must set the state of the chassis to *performanceloggingon* state, which begins the polling process. Complete the following steps to start performance logging:

Step 1 Right-click the chassis object or objects on which you want to set performance logging on.

Step 2 Choose **Cisco DSL Manager > Chassis > Configuration**.

The Chassis Configuration window opens. (See Figure 8-24.)

Figure 8-24 Chassis Configuration Window



Step 3 Click **Start** in the Global Performance Logging area on the lower right side of this window.

The Action Report window opens to inform you whether the logging process has successfully started or failed. If a failure occurs, it is often because performance logging has already been set to on.

Viewing DS3/E3 or OC-3 Interface Performance Data

This section includes the following topics:

- Performance Window Line Chart Tab, page 8-53
- Performance Window Bar Chart Tab, page 8-54
- Performance Window Table Display Tab, page 8-55
- Missed Polls, page 8-55

Note Before you can monitor performance data on any interface, you need to set global performance logging to on in the Chassis Configuration window. Right-click the chassis (DSLAM) object whose interfaces you want to monitor, and then choose **Cisco DSL Manager > Chassis > Configuration**. Click **Global Performance Logging** in the Chassis Configuration window to start logging performance data.

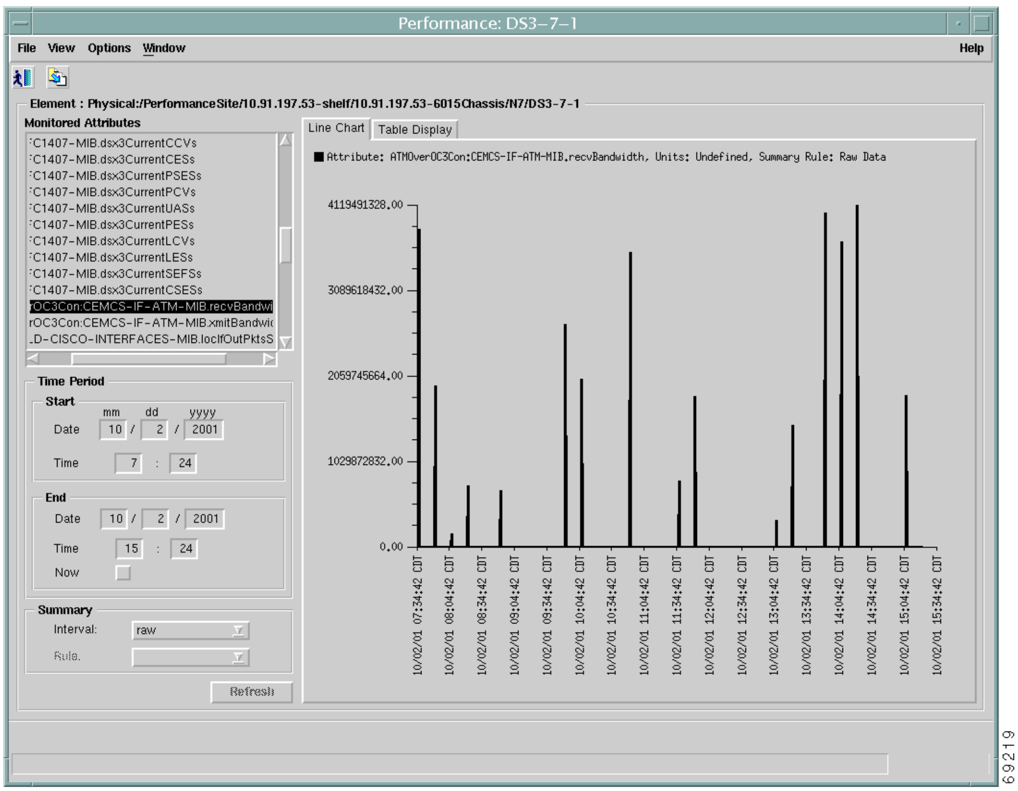
You can open the Performance Manager within the Map Viewer window. After you open the Map Viewer window, complete the following steps:

Step 1 In the Map Viewer window, within the Physical view, right-click the DS3/E3 or OC-3 interface whose performance you want to view.

Step 2 Choose **Tools > Performance Manager** from the object menu.

The Performance window opens to the Line Chart tab and displays historical performance data about the DS3/E3 interface. (See Figure 8-25.)

Figure 8-25 DS3/E3 Performance Window—Line Chart Tab



The DS3/E3 Interface Performance window consists of three left areas, and three tabbed sections at right. Choose the parameters you want from the left areas.

Step 3 From the Monitored Attributes list, choose the attribute you want to monitor. You can choose multiple contiguous attributes in a list by holding down the Shift key and then selecting the first and last attributes in the list. You can choose multiple individual attributes by holding down the Ctrl key and clicking on individual items. Information for all selected attributes is shown in the table display. Only the first selected attribute is shown in the line chart or bar chart.

In the Time Period area, choose the time parameters.

Step 4 Set the Start Date. Enter the date on which you want to begin viewing performance data in the Start Date entry boxes. The format must be mm/dd/yyyy.

Step 5 Set the Start Time. Enter the time you want the performance data to start on in the Start Time data entry boxes. Set a start time and an end time using the 24 hour clock notation. The times are inclusive.

Step 6 Set the End Date. You have two options when setting the end date. Enter the date on which you want to stop viewing performance data in the End Date entry boxes. The format must be mm/dd/yyyy. Or, select the **Now** check box to view the data from the selected start date to the current time. By selecting this option, you do not need to update the End Date and Time fields.

Step 7 Set the End Time. You have two options when setting the end time. Enter the end date on which you wish to stop viewing performance data in the End Time entry boxes. The format must be mm/dd/yyyy. Or, select the **Now** check box to view the data from the selected start date to the current time. By selecting this option, you do not have to update the end date and time fields.

Step 8 From the drop-down list, choose the summary interval. The summary interval is the period of time over which the rule is applied. This varies according to the attribute selected. You can choose the **Raw** option, which displays performance data in its most detailed format, not summarized.

Note If you choose the **Raw** option, the bar chart view is not available, and the Summary Rule option is dimmed.

Step 9 Click **Refresh**.

Refreshing the screen initiates your request for data. The text “Refresh Screen” is blue when you can refresh a screen and dimmed when this function is unavailable. Refresh Screen is available for selection when Now is selected or when any criteria have changed and you have moved the cursor away from the changed value (for example, by pressing the **Tab** key or by using the mouse).

A line chart of the performance information you requested appears on the right side of the Performance window. You can click any of the three tabs to display your data differently.

Note The performance information corresponds to the attribute raw values. If you select a summary period, the information is displayed according to the summary rule. No summary period is associated with raw data.

Performance Window Line Chart Tab

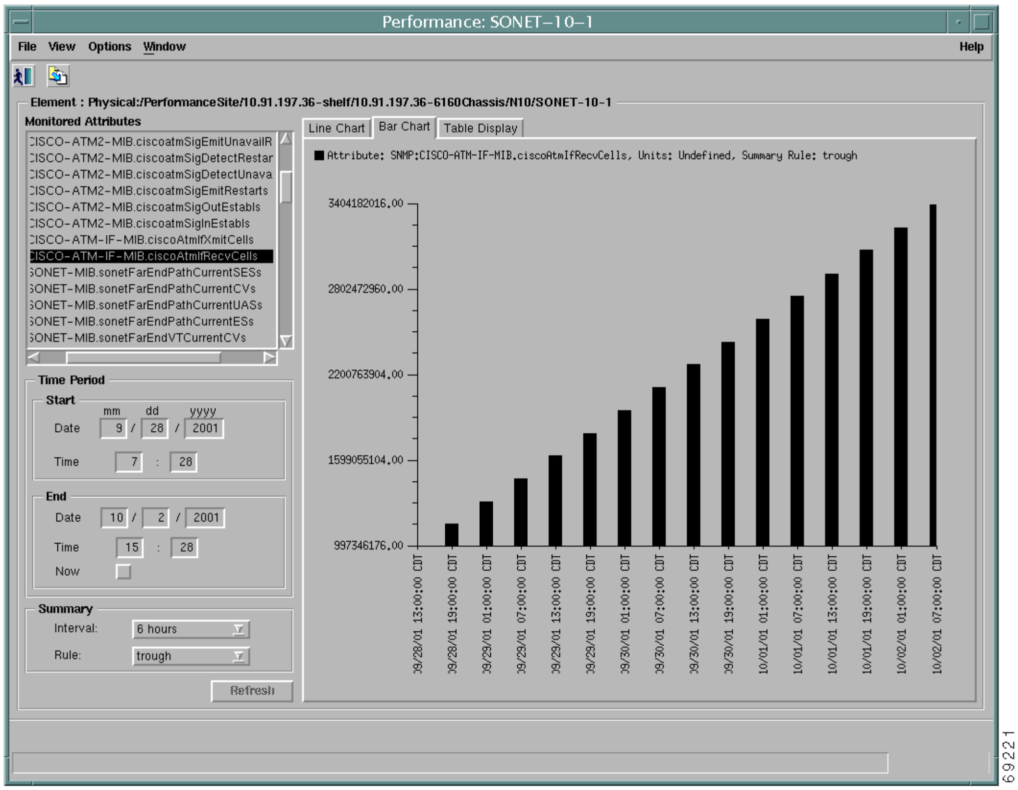
The Line Chart tab (see Figure 8-25) displays the retrieved data in a graphical format. The X-axis depicts the time at which the polling was done, and the Y-axis depicts the value retrieved or the value when the equipment did not respond properly.

Further information regarding the element, units, and missed polls is provided, using the appropriate color coding displayed at the top of the chart. Blue represents the values retrieved and red identifies any polled values missed.

Performance Window Bar Chart Tab

The information in this tab (see Figure 8-26) displays the retrieved data as a bar chart. Blue represents the values retrieved and red identifies any polled values missed.

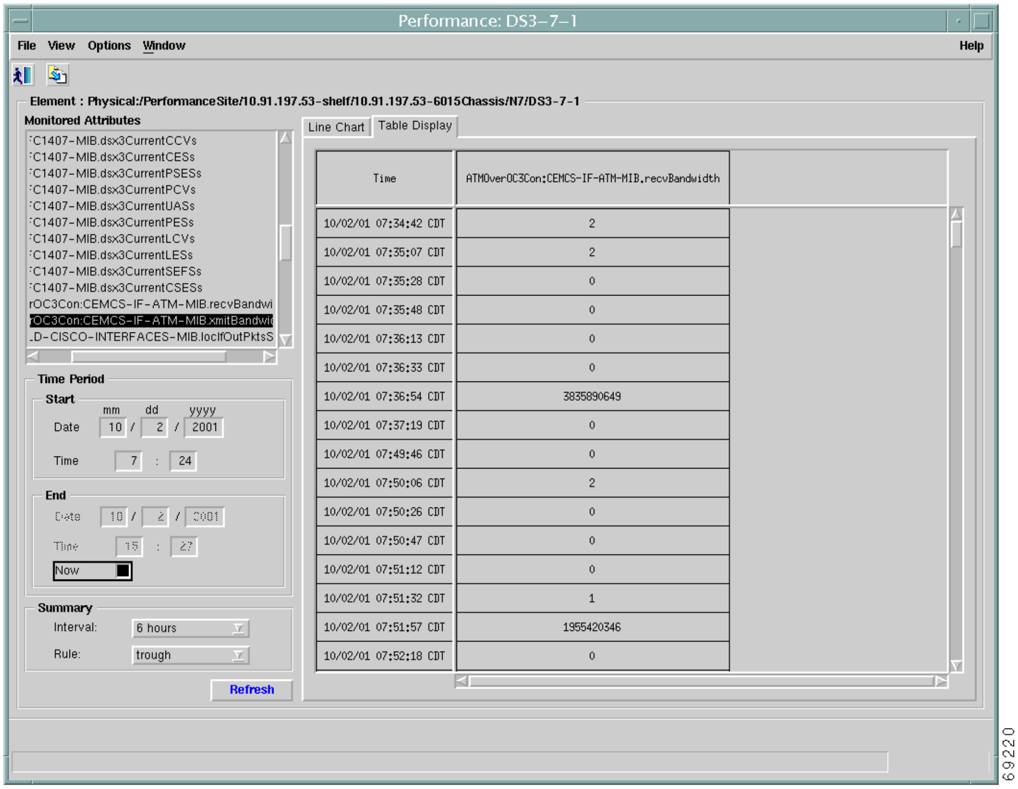
Figure 8-26 Performance Window Bar Chart Tab



Performance Window Table Display Tab

This tab (see Figure 8-27) displays the data retrieved in a tabular format. The first column shows the time of polling, and the second column shows the retrieved values. Blue represents the values retrieved and red identifies any polled values missed.

Figure 8-27 Performance Window—Table Display Tab



Missed Polls

In some circumstances, possibly due to Cisco EMF being shut down or heavy network loads, an object might fail to be monitored. This is known as a missed poll. All missed polls are indicated by a yellow point on Performance Manager graphs and charts. The last valid value collected is shown. A missed poll affects the summary data and you should not rely upon such data.

Performance Manager graphs and charts also indicate when an attribute started and stopped being polled due to history storage criteria being added, edited, or removed. Start and stop polling events are shown in charts and tables. The start polling events point is shown in green, and the stop polling events point is shown in red.

Note A polling events key appears for a selection.

Viewing ATM over ADSL over DMT Interface Performance Data

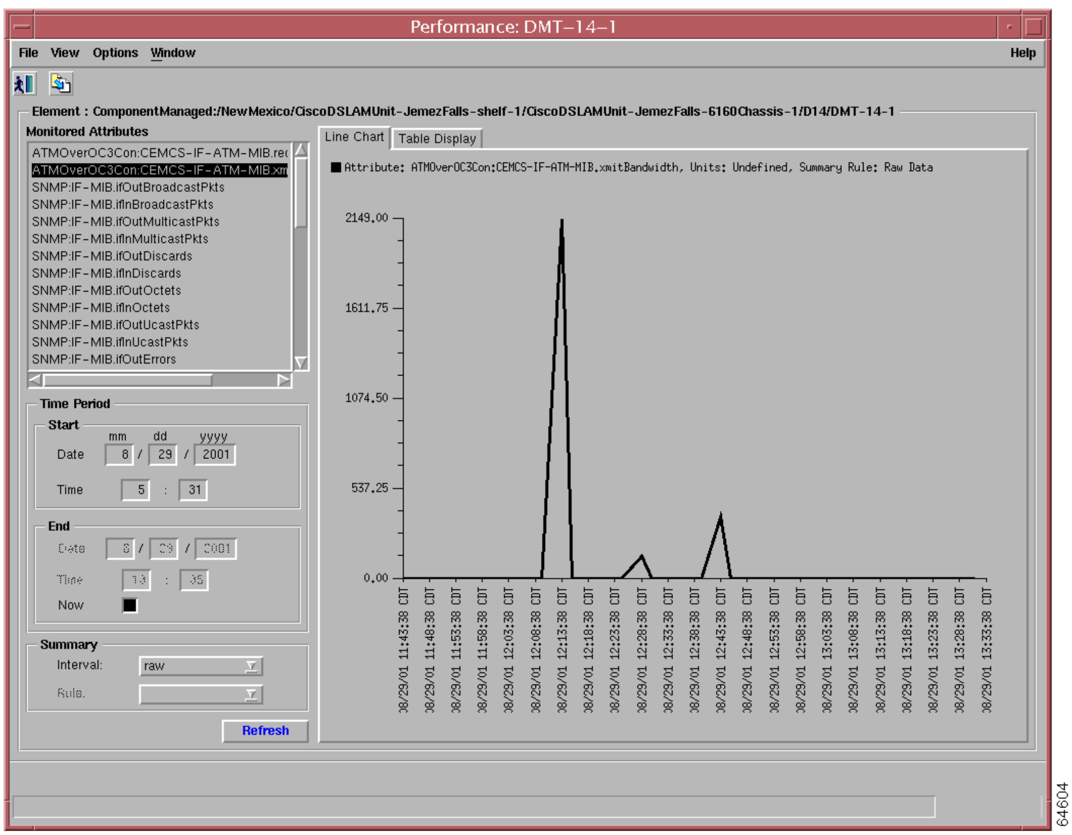
When you deploy a DMT line card, four ATM over ADSL over DMT interfaces are created automatically. For simplification, these interfaces are generally referred to as DMT interfaces throughout CDM. In a sense, the three technologies are combined in one interface. You can view performance information for any one of these technologies by selecting the one desired in the Performance Manager list box.

Step 1 In the Map Viewer window, within the Physical view, right-click the DMT interface whose performance you want to view.

Step 2 Choose **Tools > Performance Manager** from the object menu.

The Performance Manager window opens to the Line Chart tab. (See Figure 8-28.)

Figure 8-28 DMT Interface Performance Window—Line Chart Tab



The Performance Manager window consists of three areas on the left, and three tabbed sections on the right. Choose the parameters you want from the areas on the left.

Step 3 From the Monitored Attributes list, choose the attribute you want to monitor.

This list includes attributes for ATM, ADSL, and DMT interfaces. You can choose multiple contiguous attributes in a list by holding down the Shift key and then selecting the first and last attributes in the list. You can choose multiple individual attributes by holding down the Ctrl key and clicking on individual items. Information for all selected attributes is shown in the table display. Only the first selected attribute is shown in the line chart or bar chart.

Step 4 In the Time Period area, choose the time parameters.

Step 5 Set the Start Date, as follows:

Enter the date on which you want to begin viewing performance data in the Start Date entry boxes. The format must be mm/dd/yyyy.

Step 6 Set the End Date.

You have two options when setting the end date. Enter the date on which you want to stop viewing performance data in the End Date entry boxes. The format must be mm/dd/yyyy. Or, select the **Now** check box to view the data from the selected start date to the current time. By selecting this option, you need not update the end date and time fields.

Step 7 Set the Start Time.

Enter the time when you want the performance data to start in the Start Time data entry boxes. Set a start time and an end time using the 24 hour clock notation. The times are inclusive.

Step 8 Set the End Time.

You have two options when setting the end time. Enter the end date on which you wish to stop viewing performance data in the End Time entry boxes. The format must be mm/dd/yyyy. Or, select the **Now** check box to view the data from the selected start date to the current time. By selecting this option, you do not have to update the end date and time fields.

Step 9 From the drop-down list, select the summary interval.

The summary interval is the period of time over which the rule is applied. This varies according to the attribute selected. You can choose the **Raw** option, which displays performance data in its most detailed format, not summarized.

Note If you choose the Raw option, the bar chart view is not available, and the Summary Rule option is dimmed.

Step 10 Click **Refresh**.

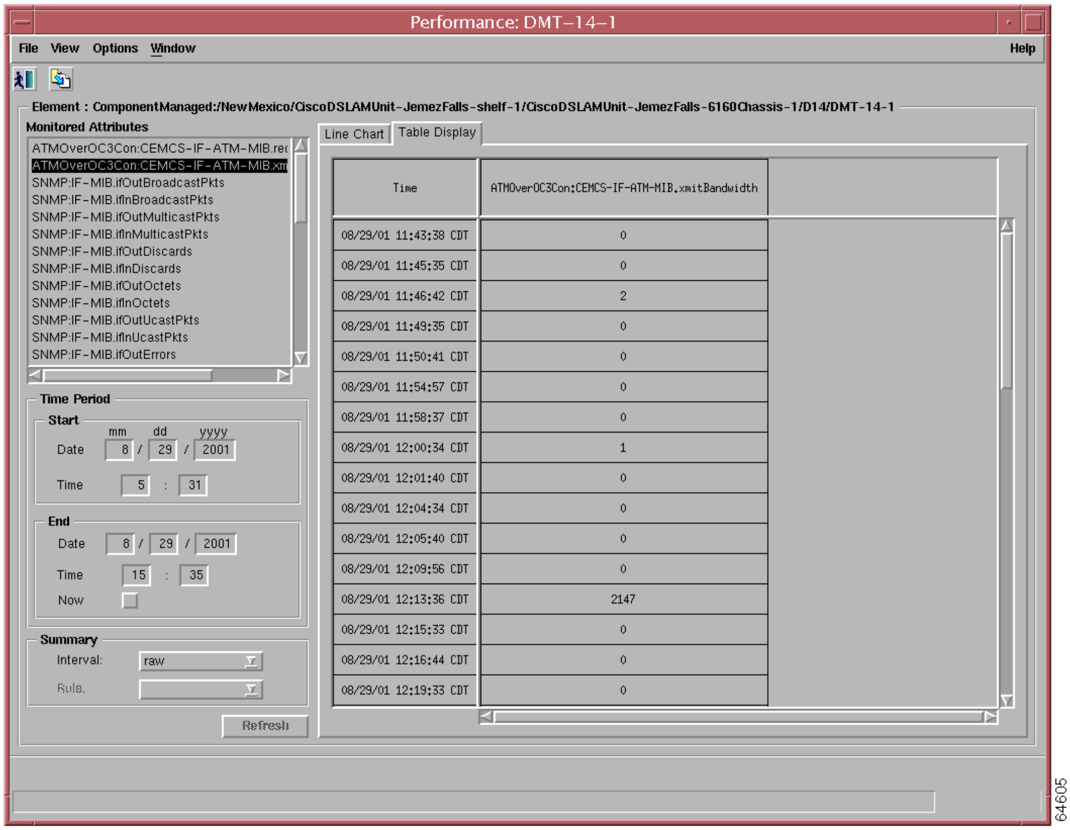
Refreshing the screen initiates your request for data. The text “Refresh Screen” is blue when you can refresh a screen and dimmed when this function is unavailable. Refresh Screen is available for selection when Now is selected or when any criteria have changed and you have moved the cursor away from the changed value (for example, by pressing the **Tab** key or by using the mouse).

A line chart of the performance information you requested appears at the right. You can click in any of the three tabs to display your data differently.

Note The performance information corresponds to the attribute raw values. If you select a summary period, the information is displayed according to the summary rule. No summary period is associated with raw data.

The Performance window—Table Display tab displays retrieved data in a tabular format. (See Figure 8-29.)

Figure 8-29 Performance Window—Table Display Tab



Viewing Inventory and Summary Information

This chapter describes how to access inventory details about Cisco DSLAM chassis and each of the cards within the chassis. This chapter also describes the Chassis Summary Data window where you can view summary information about chassis, modules, PVCs, subscribers, and other managed objects. Additionally this chapter describes the Interface Summary window through which you can view data about specific interfaces.

This chapter includes the following sections:

Viewing Chassis and Card Inventory Information

You can view inventory information about a Cisco DSLAM and the cards in the DSLAM. You view the inventory information through the Chassis Inventory window and the Module Inventory window. The following sections describe how to open the inventory information windows:

Viewing the Chassis Inventory

You open the Chassis Inventory window to view inventory information for a selected chassis. The Chassis Inventory window has two tabs, the General tab and the Asset Tracking tab. The General tab provides general details about the specific chassis, and the Asset Tracking tab provides various identification numbers relevant to the specific chassis.

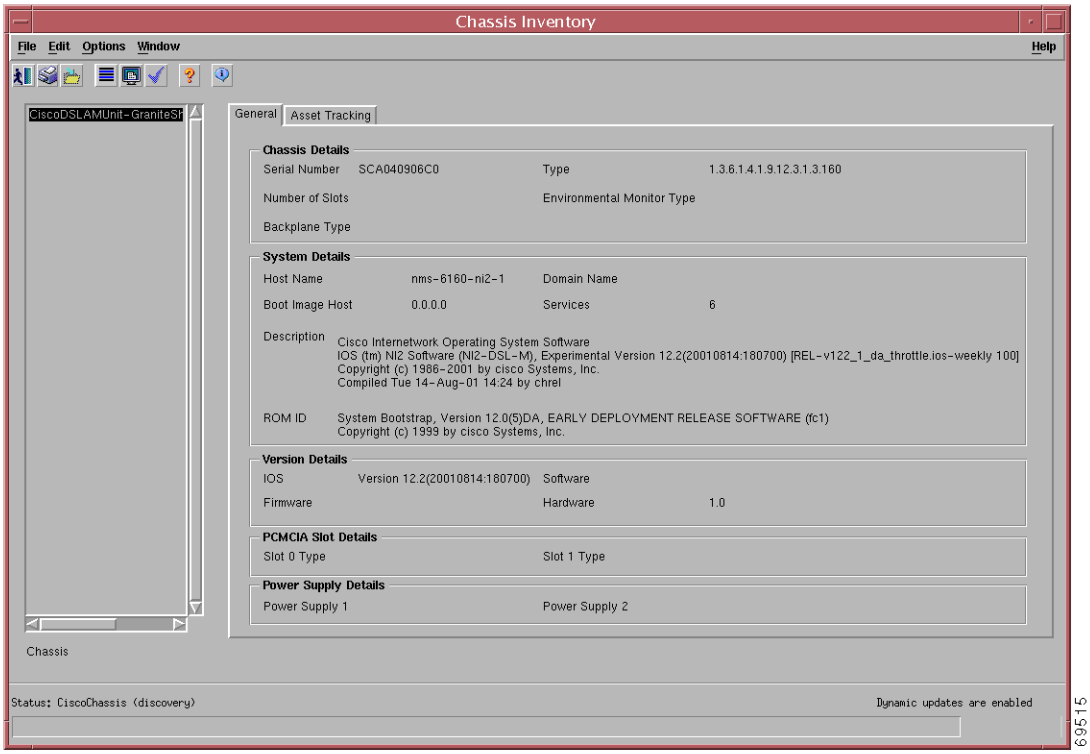
To view the Chassis Inventory window, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click the chassis whose inventory information you want to view.

Step 2 Choose **Cisco DSL Manager > Chassis > Inventory** from the object menu.

The Chassis Inventory window opens. (See Figure 9-1.)

Figure 9-1 Chassis Inventory Window—General Tab



Step 3 Select a chassis from the list on the left (the first chassis object is selected by default.)

Note The General and Asset Tracking tabs are display-only.

Viewing the Chassis Inventory Window—General Tab

The General tab contains the following five areas:

- Chassis Details
- System Details
- Version Details
- PCMCIA Slot Details—Area not used.
- Power Supply Details—Area applicable only for Cisco 6260 power entry modules (PEMs).

The fields in this tab are described in Table 9-1.

Table 9-1 Chassis Inventory Window—General Tab Field Descriptions

Field	Description
Chassis Details	
Serial Number	Displays the ID of the selected chassis.
Number of Slots	Not used.
Backplane Type	Not used.
Type	Displays the chassis type.
Environmental Monitor Type	Not used.
System Details	
Host Name	Displays the host name for the selected chassis.
Boot Image Host	Displays the IP address of the host, which supplies the software currently running.
Description	Describes the IOS and Cisco EMF software type for the selected DSLAM.
ROM ID	Displays the system boot trap description and version identifier.
Domain Name	Displays the domain portion of the domain name for the host.
Services	Displays the number of services potentially offered by the selected chassis.
Version Details	
IOS	Displays the version of the Cisco IOS commands in the selected chassis.
Firmware	Not used.
Software	Not used.
Hardware	Displays the version of the selected chassis.
PCMCIA Details	
PCMCIA Slot Details	The PCMCIA Details area is not used.

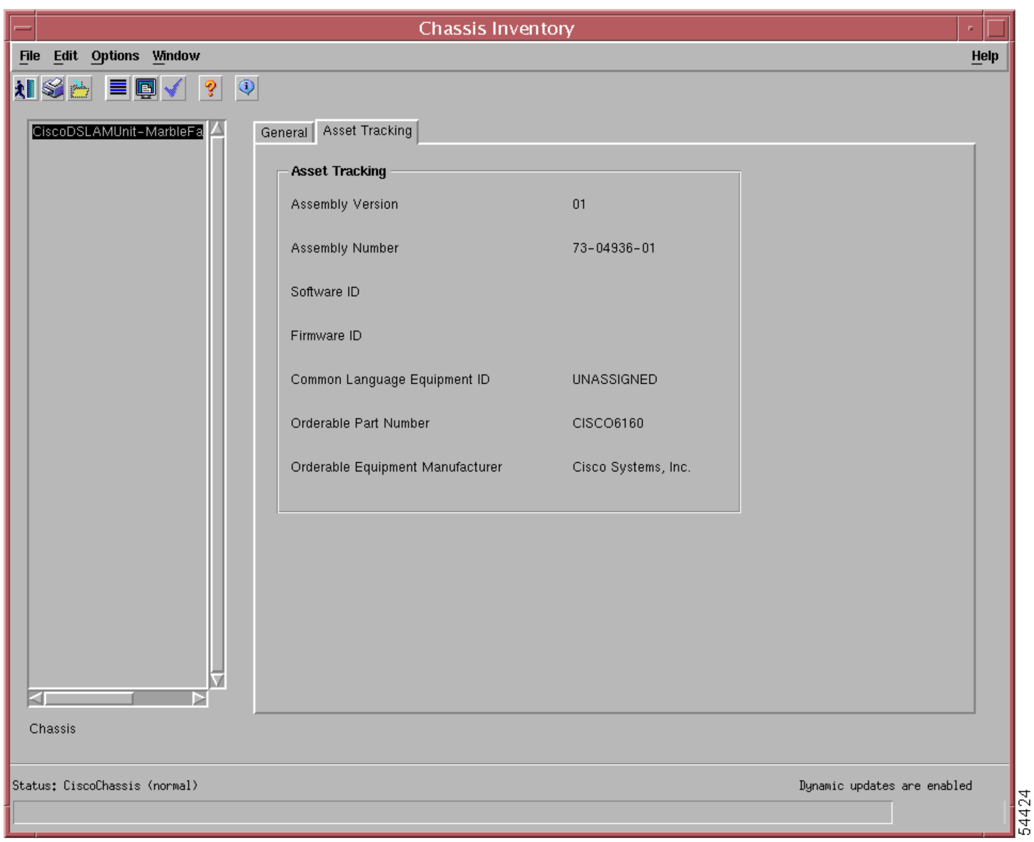
Table 9-1 Chassis Inventory Window—General Tab Field Descriptions (continued)

Field	Description
Power Supply Details	
Power Supply Details	The Power Supply Details area contains two fields—Power Supply 1 and Power Supply 2. These fields display information about the two PEMs that can be installed on a Cisco 6260 DSLAM. **Note** Refer to the *Cisco 6260 Power Entry Module FRU Installation and Replacement Notes* for detailed information about the PEMs.

Viewing the Chassis Inventory Window—Asset Tracking Tab

The Chassis Inventory Window Asset Tracking tab displays information about the hardware. (See Figure 9-2.)

Figure 9-2 Chassis Inventory Window—Asset Tracking Tab



The fields in this tab are described in Table 9-2.

Table 9-2 Chassis Inventory Window—Asset Tracking Tab Field Descriptions

Field	Description
Assembly Version	Displays the number assigned by the manufacturer that uniquely identifies the component.
Assembly Number	Displays the manufacturing assembly number, which is the hardware identification.
Software ID	Not used.
Firmware ID	Not used.
Common Language Equipment ID	Not used.
Orderable Part Number	Represents the number used to reorder this component (part number).
Original Equipment Manufacturer	Displays the original equipment manufacturer of the chassis.

Viewing the Module Inventory Window

The Module Inventory window has two tabs, General and Asset Tracking. The General tab provides general details about the specific card, and the Asset Tracking tab provides various identification numbers relevant to the specific card.

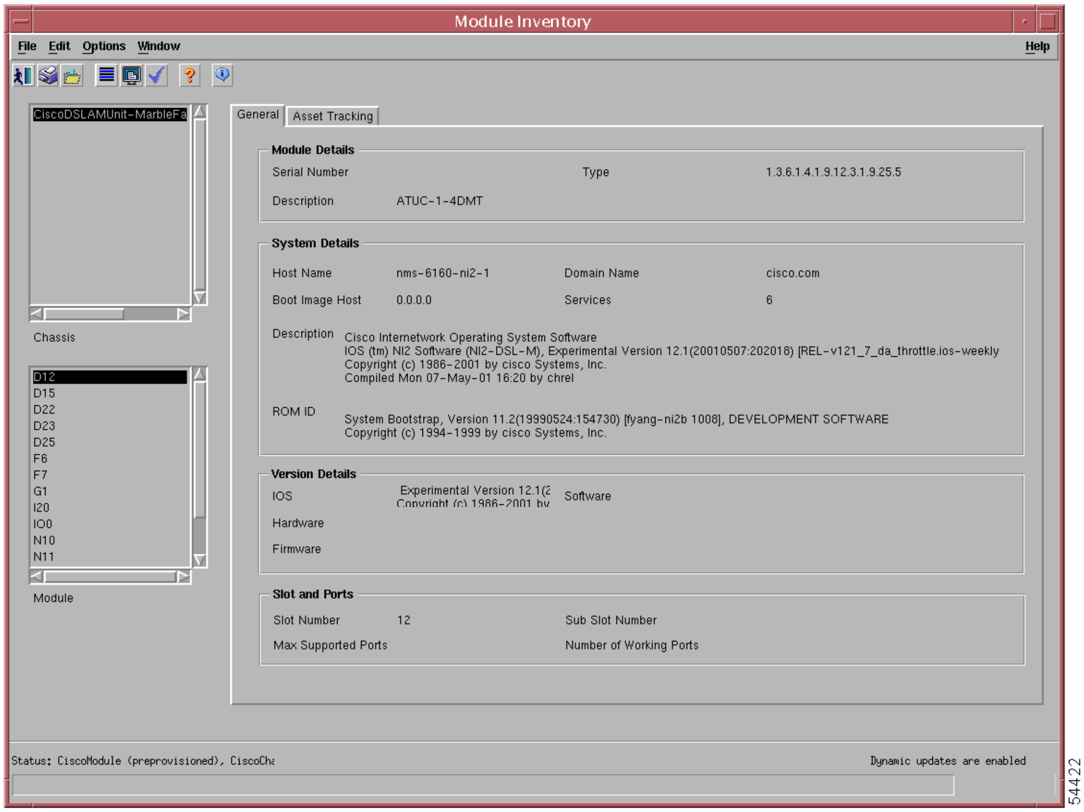
To view the Module Inventory window, complete the following steps:

Step 1 From the Map Viewer window, within the Physical view, right-click a card such as a line card or NI-2 card) whose inventory information you want to view.

Step 2 Choose **Cisco DSL Manager > Module > Inventory** from the object menu.

The Module Inventory window opens. (See Figure 9-3.)

Figure 9-3 Module Inventory Window—General Tab



The chassis and card that you selected is highlighted in the list boxes on the left side of the window. The status information for the selected card displays on the right.

Note The General and Asset Tracking tabs are display only.

Viewing the Module Inventory Window—General Tab

The General tab contains four areas:

- Module Details
- System Details
- Version Details
- Slot and Ports

The fields in this tab are described in Table 9-3.

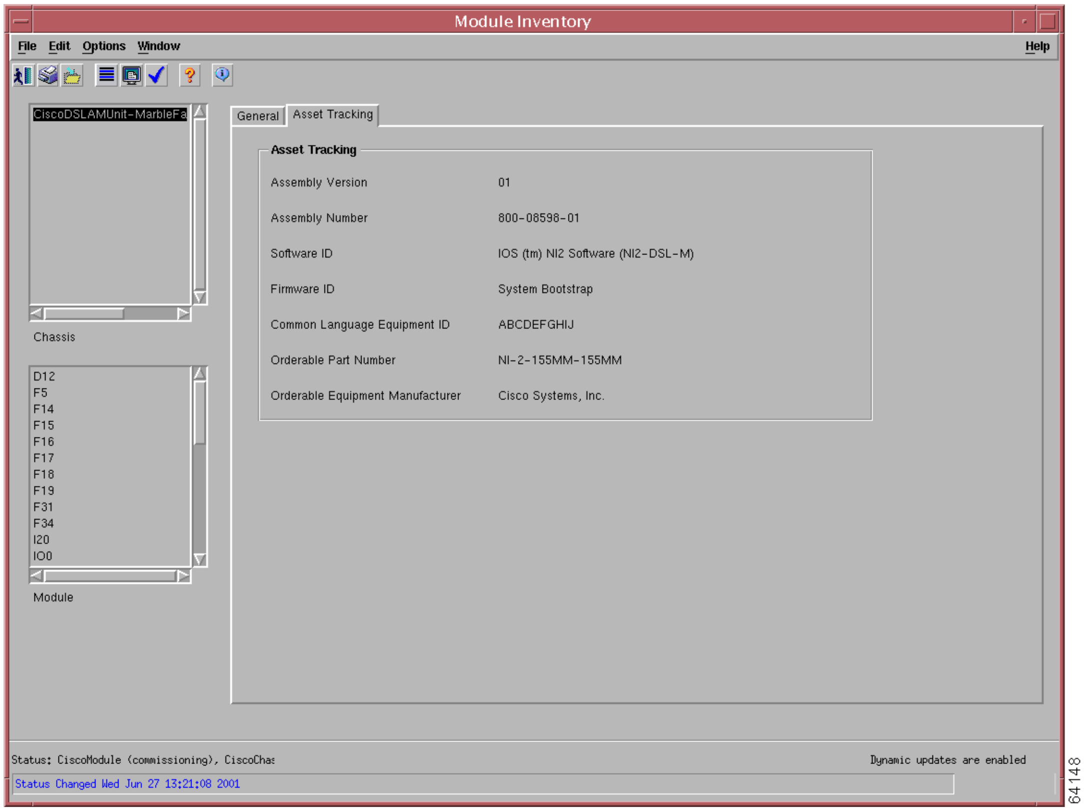
Table 9-3 Module Inventory Window—General Tab Field Descriptions

Field	Description
Module Details	
Serial Number	Displays the serial number for the selected card.
Description	Displays a description of the selected card.
Type	Displays the type of the selected card.
System Details	
Host Name	Displays the host name for the selected card.
Boot Image Host	Displays the IP address of the host, which is the source of the software that is currently running.
Description	Describes the IOS and Cisco EMF software for the selected module.
ROM ID	Displays the system boot trap description and version identifier.
Domain Name	Displays the domain portion of the domain name for the host.
Services	Displays the number of services available for the selected card.
Version Details	
IOS	Displays the version of the Cisco IOS commands in the selected card.
Hardware	Not used.
Firmware	Not used.
Software	Displays the software version installed in the card. No information appears if data is not available.
Slot and Ports	
Slot Number	Displays the current slot number location of the selected card within the chassis.
Max. Supported Ports	Not used.
Sub Slot Number	Displays the sub slot number of the selected card (not used).
Number of Working Ports	Displays the number of currently operational ports on the selected card (not used).

Viewing the Module Inventory Window—Asset Tracking Tab

The Asset Tracking tab contains one area, Asset Tracking. (See Figure 9-4.)

Figure 9-4 Module Inventory Window—Asset Tracking Tab



The fields in this area are described in Table 9-4.

Table 9-4 Module Inventory Window—Asset Tracking Tab Field Descriptions

Field	Description
Assembly Version	Displays the number assigned by the manufacturer that uniquely identifies the component.
Assembly Number	Displays the manufacturing assembly number, which is the hardware identification.
Software ID	Displays the software installed on this card.
Firmware ID	Not used.
Common Language Equipment ID	Represents the CLEI code for the card.
Orderable Part Number	Represents the number used to reorder this component (part number).
Original Equipment Manufacturer	Displays the original equipment manufacturer of the card.

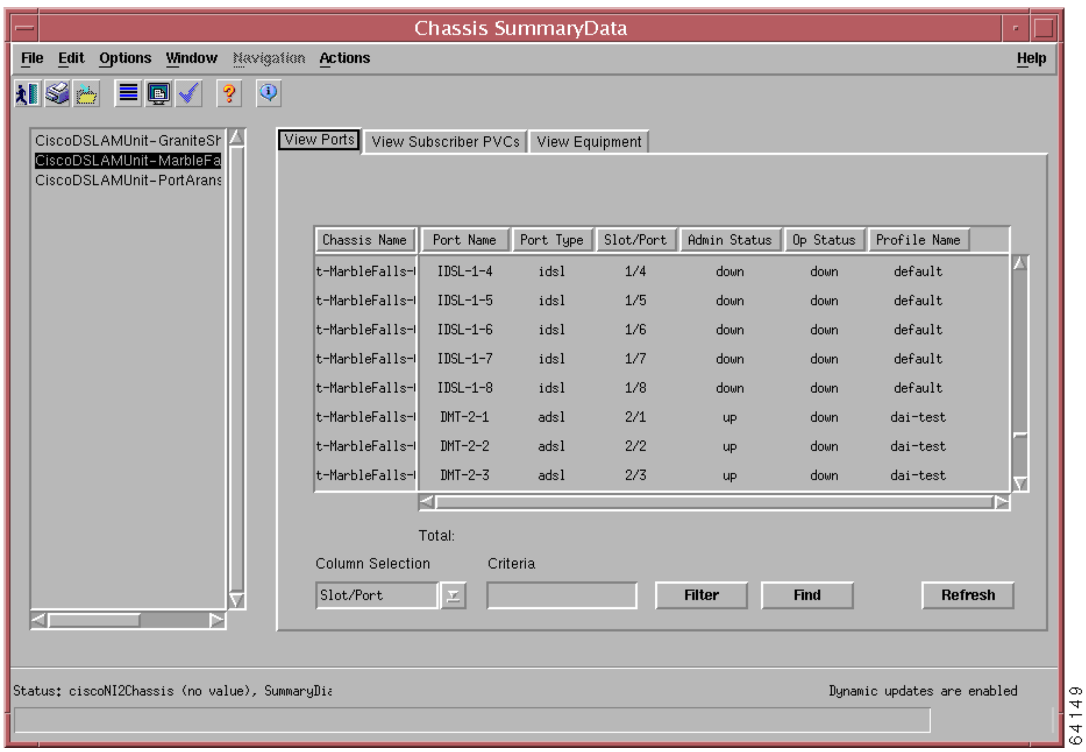
Viewing Chassis Summary Data

This section includes the following topics:

- Using the Filter Operation, page 9-10
- Using the Find Operation, page 9-10
- Using the Sort Operation, page 9-11
- Viewing Data in the Chassis Summary Data Window—View Ports Tab, page 9-11
- Viewing Data in the Chassis Summary Data Window—View Subscriber PVCs Tab, page 9-12
- Viewing Data in the Chassis Summary Data Window—View Equipment Tab, page 9-14

You can view specific data about a chassis, modules, PVCs, subscribers, and so forth in the Chassis Summary Data window. The Chassis Summary Data window is shown in Figure 9-5. You can navigate to the Chassis Summary window from a site, a shelf, or a chassis, but not from a module or an interface.

Figure 9-5 Chassis Summary Data Window—View Ports Tab



You can open the Chassis Summary Data window in three ways:

- From the site level—To view all the DSLAMs in a site
- From the shelf level—To view the summary data about one specific DSLAM and any subtended DSLAMs from within the Subtend hierarchy view
- From the chassis level—To view the summary data about one specific DSLAM

You use the same basic steps to filter and find information in each of the tabs. These steps are described in the sections that follow.

The Chassis Summary Data window has three tabs—View Ports, View Subscriber PVCs, and View Equipment—which are described in the following sections. By specifying your search criteria, you can use the Filter and Find buttons to display different types of information about specific objects. The information for the chassis that you select displays in the table in the selected tab.

Using the Filter Operation

To filter summary data about an object, complete the following steps:

Step 1 In the Column Selection field, use the down arrow to select the object type and column name that you want to filter.

Step 2 In the Criteria field, enter the alphanumeric character on which you want to filter, for example enter DMT to filter for DMT line cards.

You can enter one or more characters in the Criteria field. For example, if you are looking for the words composition, compound, or compost, you can enter either **c**, **co**, **com**, or **comp**; all three words would remain visible in the display area. Only words such as concrete or contact would display if you enter only **c** or **co**.

Note The filter is case sensitive.

Step 3 Click **Filter**.

The Chassis Summary Data window displays only the objects that match your selection in the Column Selection field based on the criteria that you entered in the Criteria field. Data displays in alphanumeric and ascending order.

Using the Find Operation

You can search more specifically by using the **Find** button, as follows:

Step 1 In the Column Selection field, use the down arrow to select the object type and column name that you want to find.

Step 2 In the Criteria field, enter the alphanumeric character for which you want to search; for example, you might enter a hardware revision number to search all chassis that have that hardware revision.

The Criteria field operates in the same way for both the Filter and the Find operations.

Step 3 Click **Find**.

The Chassis Summary Data window highlights the first record that matches that criteria in the designated column at the top of the table.

Step 4 Continue to click **Find** to display subsequent records that match the specified criteria.

Once the display reaches the bottom of the list, it starts over.

Using the Sort Operation

You can sort the data by pressing any of the column headings. In most of the columns, sorting is in ascending alphanumeric order. The Chassis column sorts the data in the original order that the server sent the data to the client.

Viewing Data in the Chassis Summary Data Window—View Ports Tab

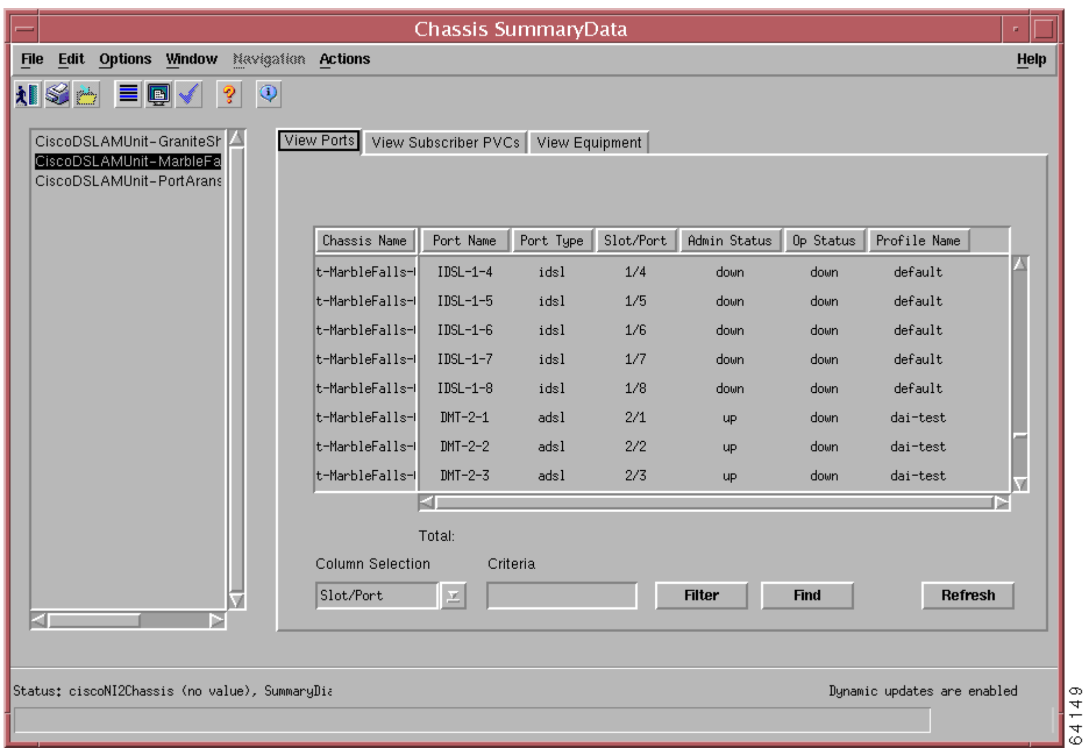
Complete the following steps to open the Chassis Summary Data window and view data about specific ports:

Step 1 From the left side of the Map Viewer window, right-click the site, shelf, or chassis object for which you want to view summary data.

Step 2 Choose **Cisco DSL Manager > Chassis > Chassis Summary** from the object menu.

The Chassis Summary Data window opens to the View Ports tab. (See Figure 9-6.)

Figure 9-6 Chassis Summary Data Window—View Ports Tab



If you opened the Chassis Summary window from a site, all of the DSLAMs for that site display in the list box on the left side of the window.

To filter, find, or sort the data, see the "Using the Filter Operation" section on page 9-10, the "Using the Find Operation" section on page 9-10, and the "Using the Sort Operation" section on page 9-11.

The View Ports tab contains data under the following column names:

- Chassis Name—Displays summary data about selected DSLAM
- Port Name—Displays summary data about selected port
- Port Type—Displays summary data about selected interface
- Slot/Port—Displays summary data about selected port or slot
- Admin Status—Displays summary data about the administrative status of the selected object
- Op Status—Displays summary data about the operational status of the selected object
- Profile Name—Displays summary data about the selected type of *x*DSL profile

When you click **Refresh**, CDM retrieves information about the selected DSLAM or DSLAMS from the server and displays that information in the window. CDM caches the data locally so that you can filter and find information quickly. The original display of the data is sorted by chassis ID in the Chassis Name column.

Viewing Data in the Chassis Summary Data Window—View Subscriber PVCs Tab

Complete the following steps to view data in the View Subscriber PVCs tab:

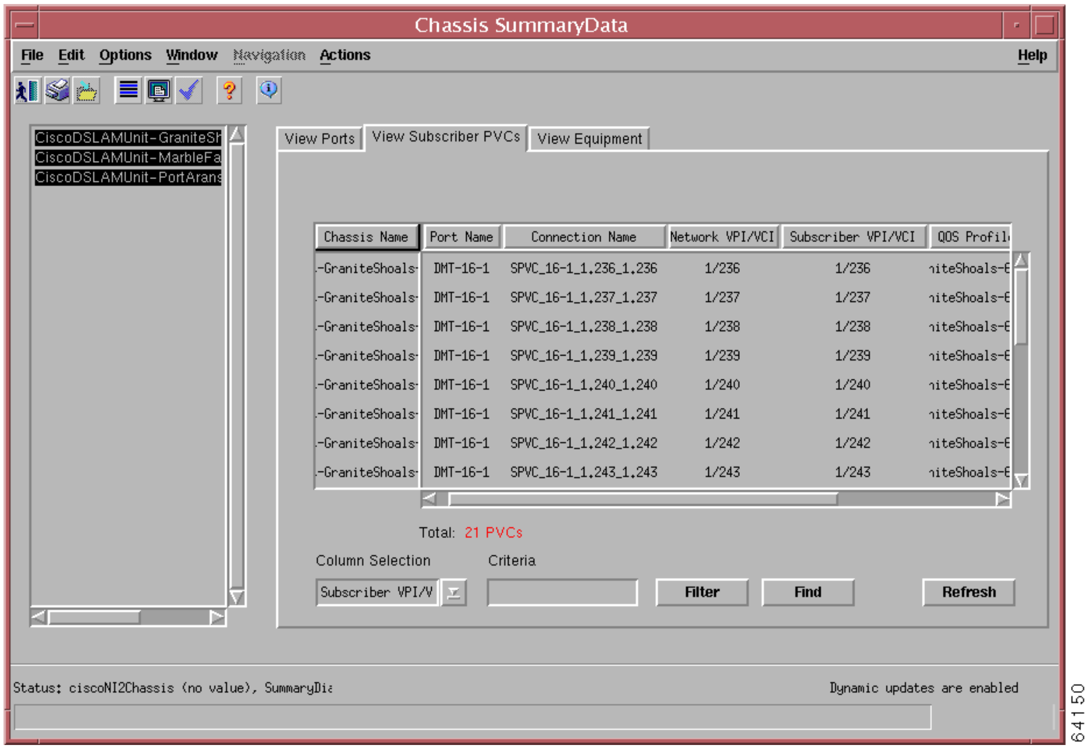
Step 1 From the left side of the Map Viewer window, right-click the site, shelf, or chassis object for which you want to view summary data.

Step 2 Choose **Cisco DSL Manager > Chassis > Chassis Summary** from the object menu.

The Chassis Summary Data window opens.

Step 3 Click the View Subscriber PVCs tab. (See Figure 9-7.)

Figure 9-7 View Subscriber PVCs Tab



The View Subscribers PVCS tab contains data that is represented by the following column names:

- Chassis Name—Displays summary data about selected DSLAM
- Subscriber ID—Displays summary data about the subscriber ID of the selected object
- Port Name—Displays all ports
- Connection Name—Displays the PVC name
- Network VPI/VCI—Displays summary data about the network side virtual path identifier or virtual channel identifier
- Subscriber VPI/VCI—Displays summary data about the subscriber side virtual path identifier or virtual channel identifier
- QoS Profile—Displays summary data about the quality of service profile for the selected object
- DLCI—Displays summary data about the data link connection identifier for the selected object
- NSAP Address—Displays summary data about the network service access point for the selected object

To filter, find, or sort the data, see the "Using the Filter Operation" section on page 9-10, the "Using the Find Operation" section on page 9-10, and the "Using the Sort Operation" section on page 9-11.

Viewing Data in the Chassis Summary Data Window—View Equipment Tab

Complete the following steps to open the Chassis Summary Data window and view data about specific ports:

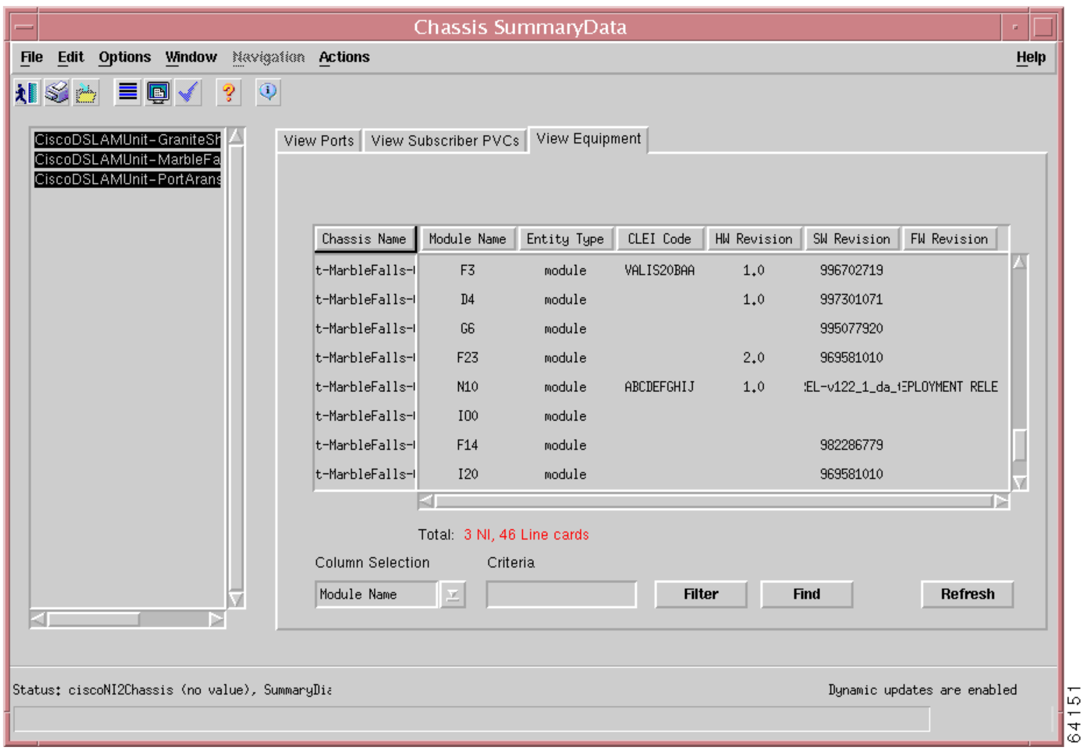
Step 1 From the left side of the Map Viewer window, right-click the site, shelf, or chassis object for which you want to view summary data.

Step 2 Choose **Cisco DSL Manager > Chassis > Chassis Summary** from the object menu.

The Chassis Summary Data window opens.

Step 3 Click the **View Equipment** tab (see Figure 9-8).

Figure 9-8 Chassis Summary Data Window—View Equipment Tab



The View Equipment tab contains data under the following column names:

- Chassis Name—Displays summary data about selected DSLAM
- Module Name—Displays summary data about the selected module
- Entity Type—Displays summary data about the entity type for the selected module
- CLEI Code—Displays summary data about the common language equipment identifier for the selected object
- HW Revision—Displays summary data about the hardware revision for the selected object
- SW Revision—Displays summary data about the software revision for the selected object
- FW Revision—Displays summary data about the firmware revision for the selected object

To filter, find, or sort the data, see the "Using the Filter Operation" section on page 9-10, the "Using the Find Operation" section on page 9-10, and the "Using the Sort Operation" section on page 9-11.

Viewing Interface Summary

You can open the Interface Summary window to view summary information about a given interface.

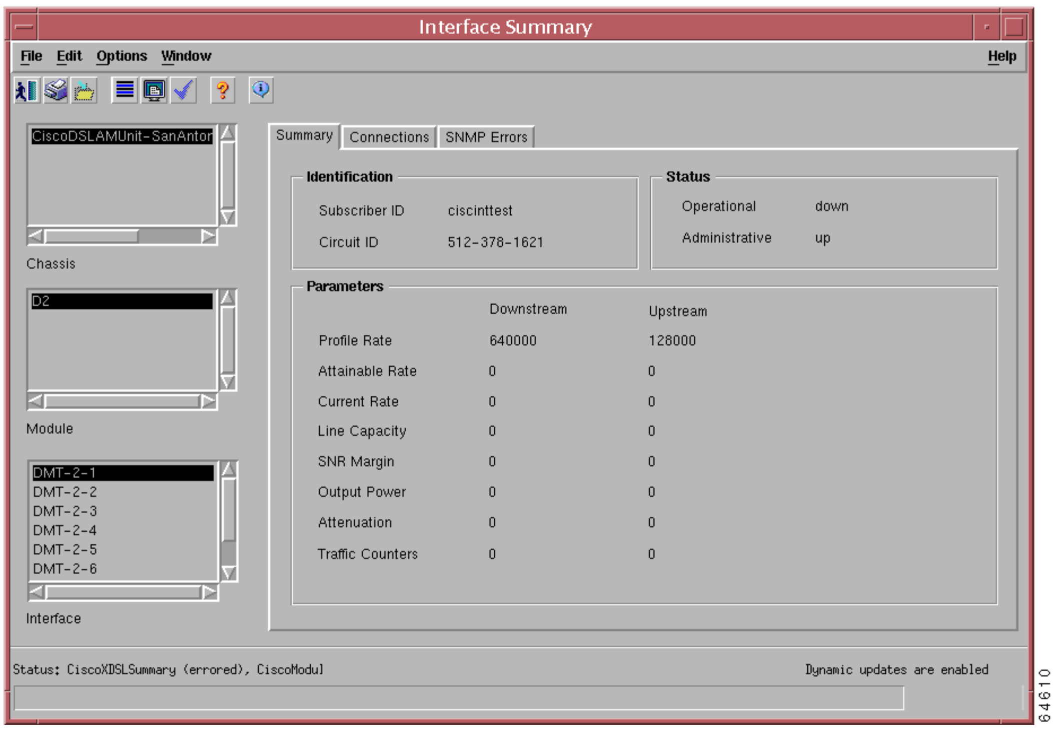
Complete the following steps to open the Interface Summary window.

Step 1 Right-click the interface whose summary data you want to view to access the object menu.

Step 2 Choose **Cisco DSL Manager > Interface > Interface Summary**.

The Interface Summary window opens. (See Figure 9-9.)

Figure 9-9 Interface Summary Window—Summary Tab



The Interface Summary window contains three tabs—Summary, Connections, and SNMP Errors. The fields in these tabs are described in the following sections.

Viewing the Interface Summary Window—Summary Tab

The Interface Summary Window Summary tab contains three areas:

- Identification
- Status
- Parameters

The fields in the Interface Summary window Summary tab are described in Table 9-5.

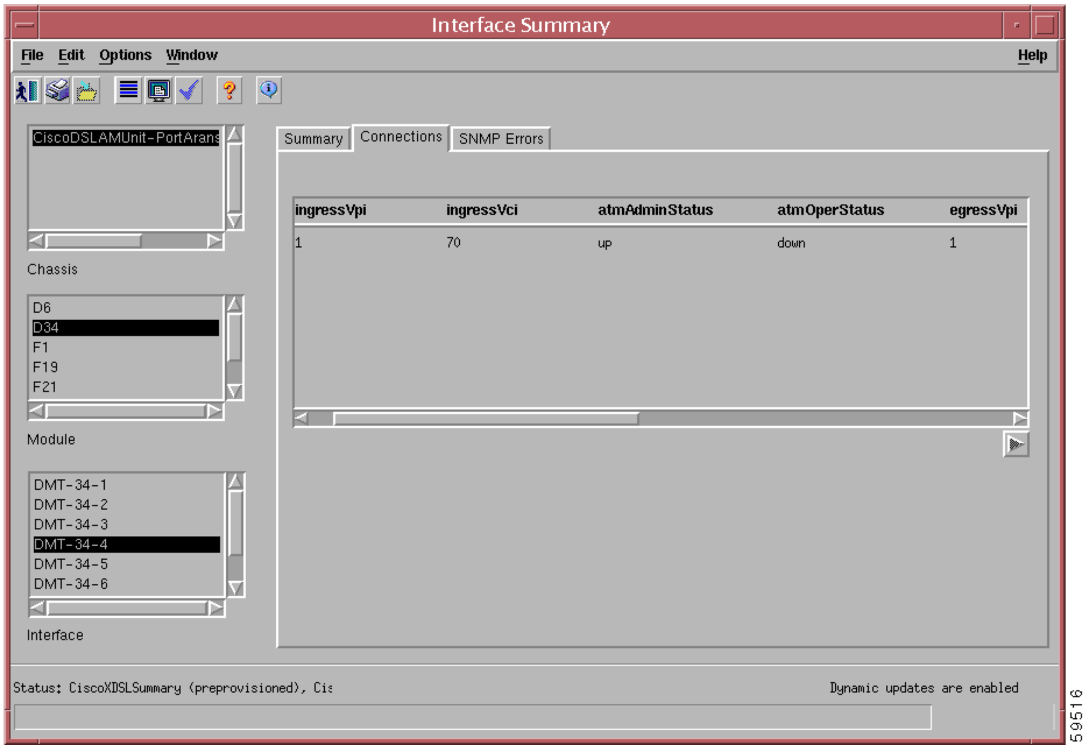
Table 9-5 Interface Summary Window—Summary Tab Field Descriptions

Field	Description
Identification	
Subscriber ID	Displays the subscriber ID associated with the interface.
Circuit ID	Displays the circuit ID associated with the interface.
Status	
Operational	Displays the operational status of the interface.
Administrative	Displays the administrative status of the interface.
Parameters	
Profile Rate	Not used.
Attainable Rate	Displays the downstream and upstream parameters of the attainable rate for that interface.
Current Rate	Displays the downstream and upstream parameters of the current rate for that interface.
Line Capacity	Displays the downstream and upstream parameters of the line capacity for that interface.
SNR Margin	Displays the downstream and upstream parameters of the signal-to-noise ratio margin for that interface.
Output Power	Displays the downstream and upstream parameters of the output power for that interface.
Attenuation	Displays the downstream and upstream parameters of the attenuation values for that interface.
Traffic Counters	Displays a count of the receive cells on the ATM interface profile rate, based on the maximum rate that is specified in the *x*DSL profile.

Viewing the Interface Summary Window—Connections Tab

The Interface Summary window Connections tab displays connections information about an interface. (See Figure 9-10.)

Figure 9-10 Interface Summary Window—Connections Tab



Use the scroll bar to scroll to each of the columns in the Connections tab. The columns in the Interface Summary window Connections tab are described in Table 9-6.

Table 9-6 Interface Summary Window—Connections Tab Column Descriptions

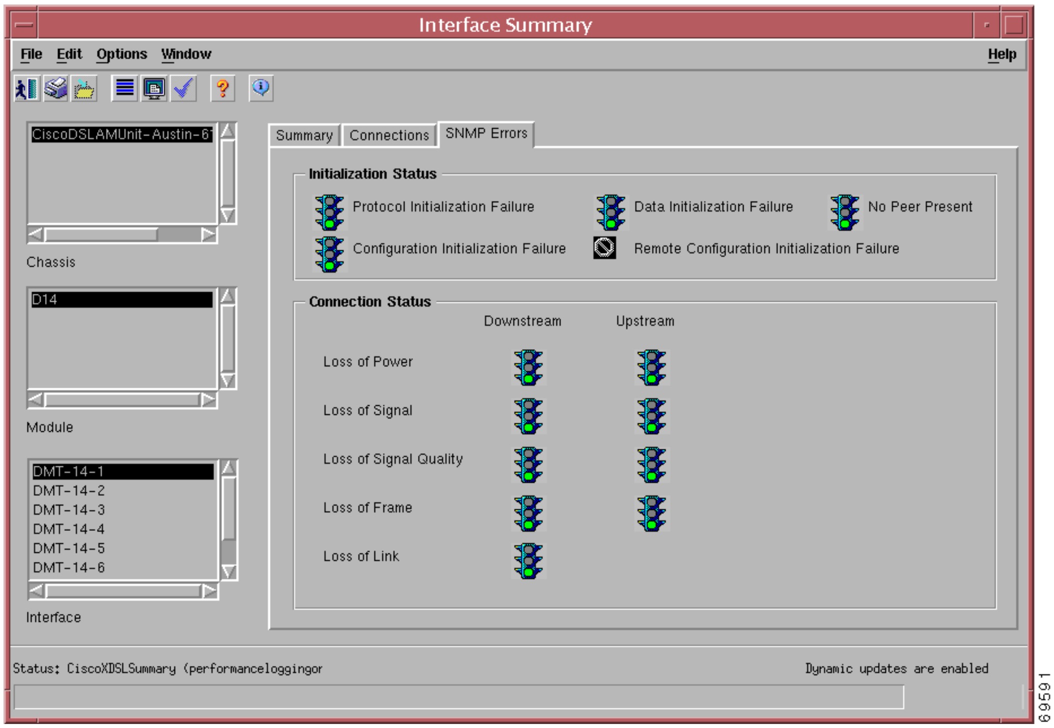
Field	Description
ingressVpi	Displays the ingress virtual path identifier for the interface.
ingressVci	Displays the ingress virtual channel identifier for the interface.
atmAdminStatus	Displays the administrative ATM status of the interface.
atmOperStatus	Displays the operator ATM status of the interface.
egressVpi	Displays the egress virtual path identifier for the interface.
egressVci	Displays the egress virtual channel identifier for the interface.
atmXConnLowPort	Identifies the cross connection for the subscriber side of the interface.
atmXConnHighPort	Displays the cross connection for the network side of the interface.
atmConftype	Displays the ATM configuration type of the interface.
profileName	Displays the QoS profile name that is applied to the interface.

Viewing the Interface Summary Window—SNMP Errors Tab

The Interface Summary window SNMP Errors tab displays information about interface SNMP errors. (See Figure 9-11.)

Note The SNMP Errors tab displays values for ADSL interfaces only, that is, CAP and DMT line cards.

Figure 9-11 Interface Summary Window—SNMP Errors Tab



The SNMP Errors tab displays traffic signal icons to indicate status. Red indicates errors; green indicates normal; yellow indicates a warning status. Table 9-7 describes the fields in the Interface Summary window SNMP Errors tab. A circle with a slash through it indicates that the field is not significant for the current conditions.

Table 9-7 Interface Summary Window—SNMP Errors Tab Field Descriptions

Field	Description
Initialization Status	
Protocol Initialization Failure	Displays red light for protocol initialization failure; displays green light if no protocol initialization failure.
Configuration Initialization Failure	Displays red light for configuration initialization failure; displays green light if no configuration initialization failure.
Data Initialization Failure	Displays red light for data initialization failure; displays green light if no data initialization failure.
Remote Configuration Initialization Failure	Displays red light for remote configuration initialization failure; displays green light if no remote configuration initialization failure.

Table 9-7 Interface Summary Window—SNMP Errors Tab Field Descriptions

Field	Description
No Peer Present Failure	Displays red light if no peer present; displays green light if peer is present.
Connection Status	
Loss of Power	Displays red light for loss of power for downstream and upstream connections; displays green light if no loss of power.
Loss of Signal	Displays red light for loss of signal for downstream and upstream connections; displays green light if no loss of signal.
Loss of Signal Quality	Displays red light for loss of signal quality for downstream and upstream connections; displays green light if no loss of signal quality.
Loss of Frame	Displays red light for loss of frame for downstream and upstream connections; displays green light if no loss of frame.
Loss of Link	Displays red light for loss of link for downstream and upstream connections; displays green light if no loss of link.

APPENDIX A

Viewing Alarms and Events

This appendix describes how to identify faults (events or alarms) that a Cisco DSLAM generates on the network. When a fault occurs on a managed object in the network, CDM receives immediate notification. When you open the Cisco EMF Event Browser from the launchpad, a color next to the network object indicates the presence of an alarm.

SNMP traps raise alarms on CDM. You can detect the source of an alarm by using the Event Browser to navigate through the network object hierarchy to the affected object. Alarms are propagated up the element hierarchy according to severity (see Table A-2). All alarms are stored within the Event Browser, which displays both current and historical data. For further information on the Event Browser, refer to the *Cisco Element Management Framework User Guide*.

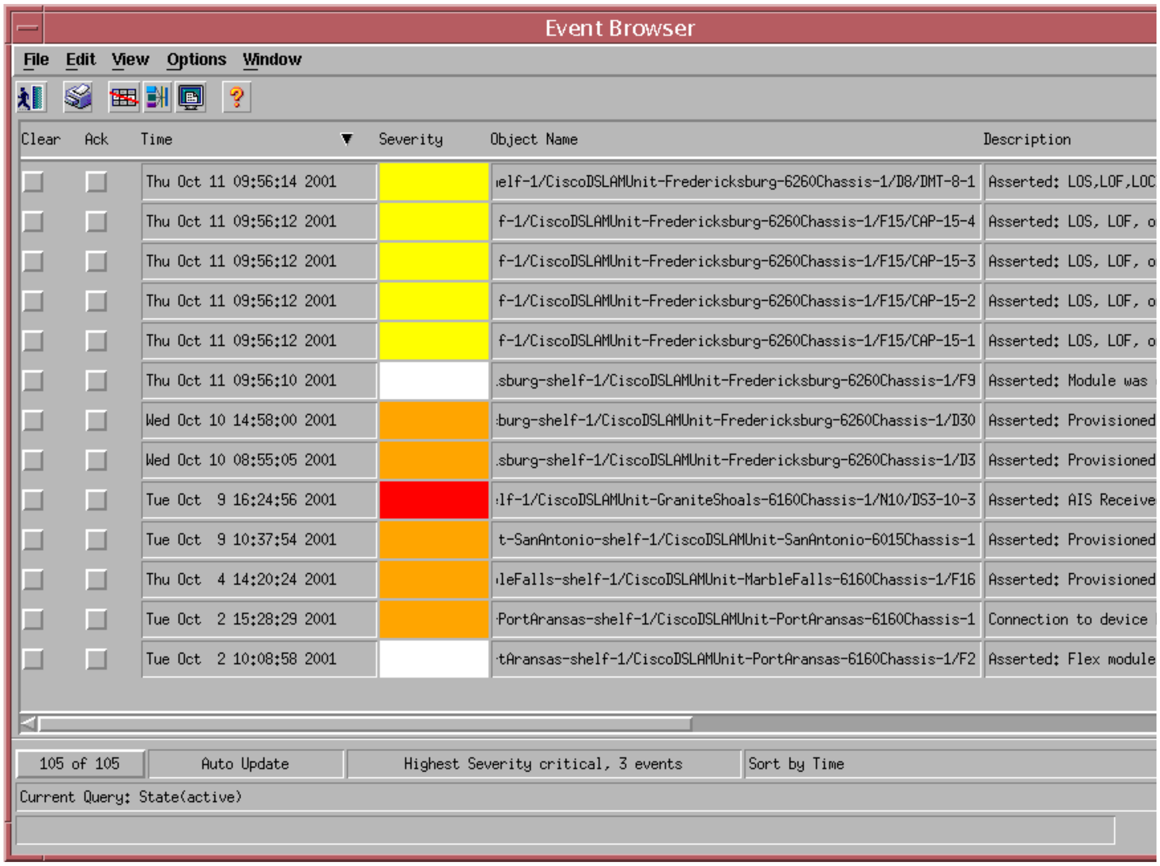
This appendix includes the following sections:

Viewing Alarms through the Event Browser Window

You can detect the source of an alarm by using the Event Browser window, or Event Browser, to navigate through the network object hierarchy to the affected object. Alarms propagate up the element hierarchy according to severity. The Event Browser displays events that the system flags.

The Event Browser window is shown in Figure A-1.

Figure A-1 Event Browser Window



The Event Browser stores all alarms and displays current as well as historical data. You can detect the presence of an alarm by the color that Cisco EMF uses to represent network objects. The color of an alarm indicates its severity. SNMP traps raise alarms on CDM.

For further information on the Event Browser, refer to the *Cisco Element Manager Framework User Guide*.

The Event Browser window displays the following information in a table format:

- In the Time column, the time and date when the system reports an event
- In the Severity column, the level of severity, indicated by the color
- In the Object Name column, the name of the object that is affected by the event
- In the Description column, a description of the event

Note Use the scroll bars to view all of the columns and all of the alarms.

You can navigate directly from a single event to the affected object to perform detailed configuration activities.

To view events in the Event Browser window, follow these steps:

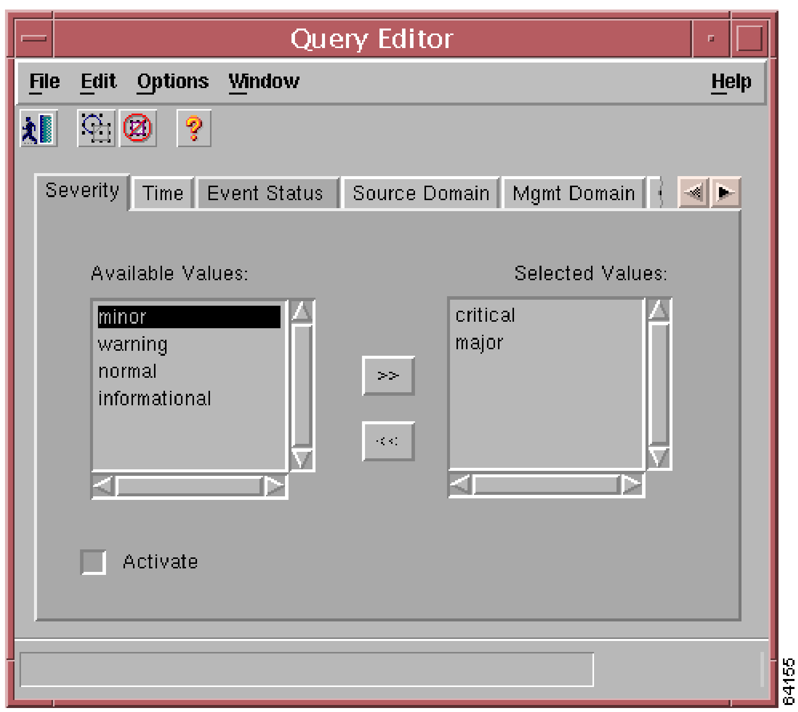
Step 1 Open the Event Browser window by using one of the following methods:

- Choose **Event Browser** from the Window menu in the CDM Map Viewer window.
- Right-click the object on the relevant chassis in the Map Viewer window.
- Right-click the object on a map node.
- Click the **Events** icon on the Cisco EMF Launchpad. (See Figure A-2.)

Figure A-2 Events Icon

If you click the **Events** icon, the Event Browser can display events for all of the DSLAMs being managed. Clicking the **Events** icon opens the Query Editor window (see Figure A-3). Through this window you can specify the severity of the alarms you want to view. (Once the Event Browser is open, you can open the Query Editor again by choosing **Query Setup** from the **Edit** menu.)

Figure A-3 Query Editor Window



Step 2 Set your query criteria on the window.

The Query Editor contains the following tabs that you can use to define and refine your alarm search criteria:

- Severity
- Time

- Event Status
- Source Domain
- Mgmt Domain
- User
- Event Class
- Object Scope
- Object Class
- Object Attribute Presence
- Object Attribute Value

Step 3 Use the >> or << arrows to select or deselect the choices in the Available Values column:

- critical
- major
- minor
- warning
- normal
- informational

Step 4 Always click **Activate** after you specify the values for the alarms that you want to view.

The Event Browser displays all alarms that match your query criteria.

Note Refer to the *Cisco Element Manager Framework User Guide* for more detailed information about using the Query Editor.

Viewing ATM Interface Faults

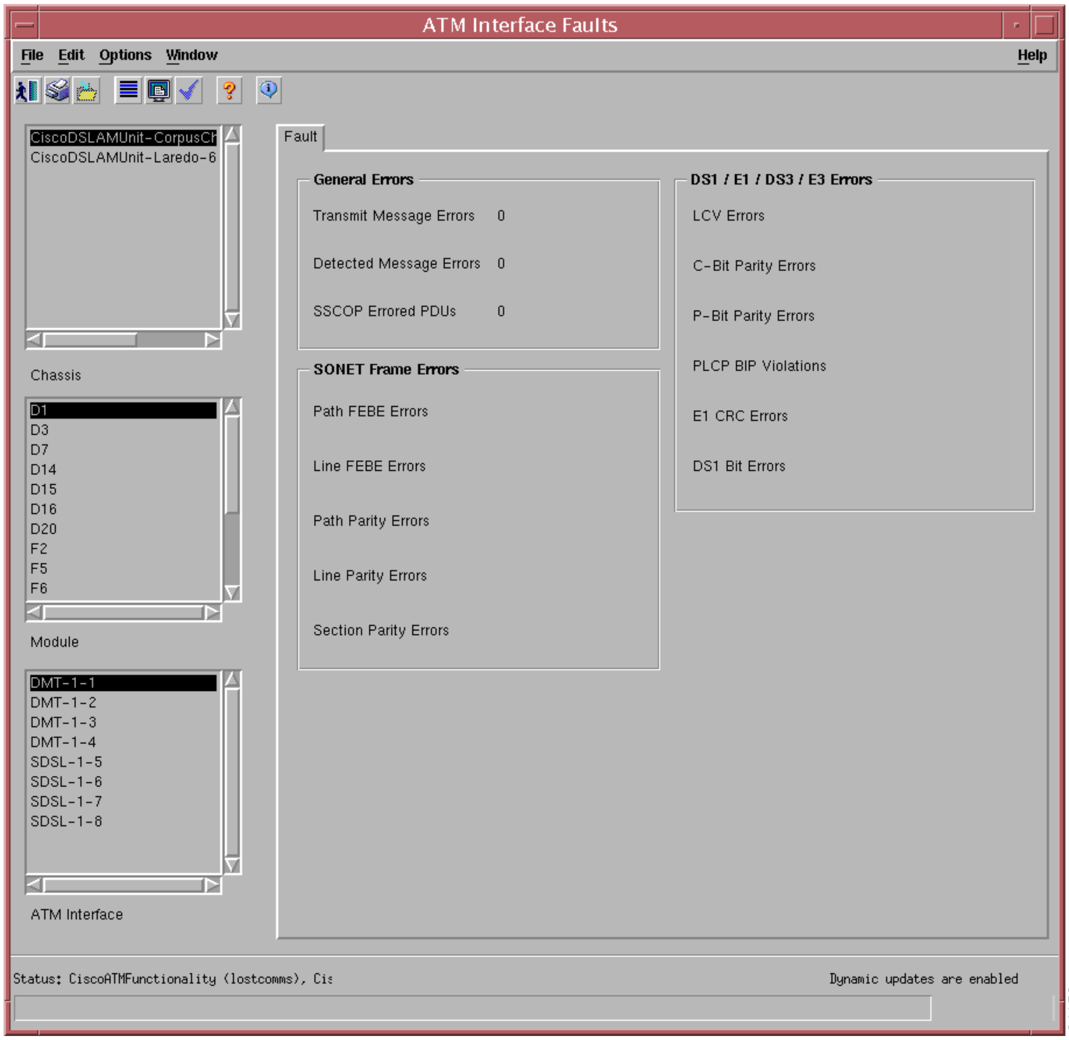
You can view faults on ATM interfaces for a specified interface. Complete the following steps to view ATM interface faults:

Step 1 From the Map Viewer window, in the Component Managed view, right-click the chassis object for which you want to view ATM interface faults to access the object menu.

Step 2 Choose **Cisco DSL Manager > Interface > Faults > ATM**.

The ATM Interface Faults window opens. (See Figure A-4.)

Figure A-4 ATM Interface Faults Window



Step 3 From the list boxes on the left, select the relevant chassis, card, and ATM interface.

The fault information for the selected ATM interface appears in the Fault tab on the right.

The Fault tab consists of three areas:

- General Errors
- SONET Frame Errors (not applicable to Cisco DSLAMs)
- DS1/E1/DS3/ E3 Errors (not applicable to Cisco DSLAMs)

Table A-1 describes the fields in these areas.

Table A-1 ATM Interface Window—Fault Tab Field Description

Field	Description
General Errors	
Transmitted Message Errors	Specifies the number of Incorrect Messages transmitted on the interface. The Incorrect Messages counter reflects any sort of incorrect information in a message.
Detected Message Errors	Identifies the number of Incorrect Messages detected on the interface. The Incorrect Messages counter reflects any sort of incorrect information in a message.
SSCOP Errored PDUs	Calculates the sum of the following errors—Invalid PDUs are defined in SSCOP and consist of PDUs with incorrect length (MAA-ERROR code U); undefined PDU type code; or not 32-bit aligned. PDUs that result in MAA error codes are discarded.
SONET Frame Errors	This area not used.
DS1/E1/DS3/E3 Errors	This area not used.

Determining Alarm Severity

The possible alarm colors and the alarm severity that each color represents is described in Table A-2.

Table A-2 Severity Colors

Color	Severity of Alarms
Red	Critical
Orange	Major
Brown	Moderate
Yellow	Minor
Cyan	Warning
Green	No alarms (normal)
Blue	Card decommissioned or not installed
White	Informational
Dark Green	Preprovisioned

Identifying CDM Alarms

The tables in this section list the alarms that are related to the Cisco Entity Alarm MIB.

This section contains the following sections:

Cisco 6100 Alarms

Table A-3 describes alarms specific to the Cisco 6100 DSLAM.

Table A-3 Cisco 6100 Alarms

Alarm Severity	Description	Asserted	Cleared
Major	Chassis temperature too high	When the chassis inlet temperature is greater than or equal to 50°C, or when the chassis outlet temperature is greater than or equal to 65°C	When the chassis inlet temperature is less than 50°C, or when the chassis outlet temperature is less than 65°C
Major	Chassis temperature too low	When the chassis inlet temperature is less than or equal to –40°C, or when the chassis outlet temperature is less than or equal to –40°	When the chassis inlet temperature is greater than –40°C, or when the chassis outlet temperature is greater than –40°C

Table A-3 Cisco 6100 Alarms (continued)

Alarm Severity	Description	Asserted	Cleared
Major	Temperature rating mismatch	When a chassis contains at least one industrial temperature component and at least one commercial temperature component	When all components in a chassis are industrial temperature, or when all components in a chassis are commercial temperature
Major	Fan tray missing or failed	When the fan is missing or has failed	When the fan in functioning properly

Cisco 6015 Alarms

Table A-4 describes alarms specific to the Cisco 6015 DSLAM.

Table A-4 Cisco 6015 Alarms

Alarm Severity	Description	Asserted	Cleared
Major	Chassis temperature too high	When the chassis inlet temperature is greater than or equal to 50°C, or when the chassis outlet temperature is greater than or equal to 65°C	When the chassis inlet temperature is less than 50°C, or when the chassis outlet temperature is less than 65°C
Major	Chassis temperature too low	When the chassis inlet temperature is less than or equal to –40°C, or when the chassis outlet temperature is less than or equal to –40°	When the chassis inlet temperature is greater than –40°C, or when the chassis outlet temperature is greater than –40°C
Major	Temperature rating mismatch	When a chassis contains at least one industrial temperature component and at least one commercial temperature component	When all components in a chassis are industrial temperature, or when all components in a chassis are commercial temperature
Major	Fan Slot not detected or missing	When the agent does not detect the presence of a fan tray in the corresponding fan tray slot	When the agent detects the presence of a fan tray in the corresponding fan tray slot
Major	Multiple fan failures	When more than one fan contained by the fan tray has failed	When all fans contained by the fan tray are functioning properly or when a single fan contained by the fan tray has failed
Minor	Single fan failure	When a single fan contained by the fan tray has failed	When all fans contained by the fan tray are functioning properly or when more than one fan contained by the fan tray has failed
Major	Input voltage out of range	When the input voltage is less than minimum (VAC) or when the input voltage is greater than maximum (VAC)	When the input voltage is greater than or equal to minimum (VAC) and less than or equal to maximum (VAC)
Major	Excessive current	When the product of the input voltage and input current is greater than 1050 W	When the product of the input voltage and the input current is less than or equal to 1050 W

Cisco 6130 Alarms

Table A-4 describes alarms specific to the Cisco 6130 DSLAM.

Table A-5 Cisco 6130 Alarms

Alarm Severity	Description	Asserted	Cleared
Critical	Fan module not detected	When the agent does not detect the presence of a fan module	When the agent detects the presence of a fan module
Critical	Fan tray missing or failed	When the agent does not detect the presence of a fan tray	When the agent detects the presence of a fan tray
Major	Chassis temperature too high	When the chassis inlet temperature is greater than or equal to 50°C, or when the chassis outlet temperature is greater than or equal to 65°C	When the chassis inlet temperature is less than 50°C, or when the chassis outlet temperature is less than 65°C
Major	Chassis temperature too low	When the chassis inlet temperature is less than or equal to –40°C, or when the chassis outlet temperature is less than or equal to –40°	When the chassis inlet temperature is greater than –40°C, or when the chassis outlet temperature is greater than –40°C
Major	Temperature rating mismatch	When a chassis contains at least one industrial temperature component and at least one commercial temperature component	When all components in a chassis are industrial temperature, or when all components in a chassis are commercial temperature
Major	Door open alarm	Alarm generated by equipment wired to connector P4 pin 0 on the I/O card	Alarm cleared by equipment wired to connector P4 pin 0 on the I/O card

Cisco 6160 Alarms

Table A-6 describes alarms specific to the Cisco 6160 DSLAM.

Table A-6 Cisco 6160 Alarms

Alarm Severity	Description	Asserted	Cleared
Major	Chassis temperature too high	When the chassis inlet temperature is greater than or equal to 50°C, or when the chassis outlet temperature is greater than or equal to 65°C	When the chassis inlet temperature is less than 50°C, or when the chassis outlet temperature is less than 65°C
Major	Chassis temperature too low	When the chassis inlet temperature is less than or equal to –40°C, or when the chassis outlet temperature is less than or equal to –40°	When the chassis inlet temperature is greater than –40°C, or when the chassis outlet temperature is greater than –40°C
Major	Temperature rating mismatch	When a chassis contains at least one industrial temperature component and at least one commercial temperature component	When all components in a chassis are industrial temperature, or when all components in a chassis are commercial temperature

Table A-6 Cisco 6160 Alarms (continued)

Alarm Severity	Description	Asserted	Cleared
Major	Door open alarm	Alarm generated by equipment wired to connector P4 pin 0 on the I/O card	Alarm cleared by equipment wired to connector P4 pin 0 on the I/O card
Major	Station alarm 1	Alarm generated by equipment wired to connector P5 pin 1 on the I/O card	Alarm cleared by equipment wired to connector P5 pin 1 on the I/O card
Major	Station alarm 2	Alarm generated by equipment wired to connector P5 pin 3 on the I/O card	Alarm cleared by equipment wired to connector P5 pin 3 on the I/O card
Major	Station alarm 3	Alarm generated by equipment wired to connector P5 pin 2 on the I/O card	Alarm cleared by equipment wired to connector P5 pin 2 on the I/O card
Major	Fan Slot not detected or missing	When the agent does not detect the presence of a fan tray in the corresponding fan tray slot	When the agent detects the presence of a fan tray in the corresponding fan tray slot
Major	Fan fault	When the fan inside the power supply indicates a fault	When the fan inside the power supply does not indicate a fault
Major	Power supply fault	When the power supply indicates a fault	When the power supply does not indicate a fault
Major	Temperature exceeds limit	When the internal power supply temperature is greater than or equal to 50° C or when the external power supply temperature is greater than or equal to 65° C	When the internal power supply temperature is less than 50°C and the external power supply temperature is less than 65°C
Major	Not detected or missing	When the agent does not detect the presence of a fan tray in the corresponding fan tray slot	When the agent detects the presence of a fan tray in the corresponding fan tray slot
Minor	Single fan failure	When a single fan contained by the fan tray has failed	When all fans contained by the fan tray are functioning properly or when more than one fan contained by the fan tray has failed
Major	Multiple fan failures	When more than one fan contained by the fan tray has failed	When all fans contained by the fan tray are functioning properly or when a single fan contained by the fan tray has failed
Minor	Not detected or missing	When the agent does not detect the presence of a fan tray in the corresponding power supply bay	When the agent detects the presence of a fan tray in the corresponding power supply bay

Cisco 6260 Alarms

Table A-7 describes alarms specific to the Cisco 6260 DSLAM.

Table A-7 Cisco 6260 Alarms

Alarm Severity	Description	Asserted	Cleared
Major	Chassis temperature too high	When the chassis inlet temperature is greater than or equal to 50°C, or when the chassis outlet temperature is greater than or equal to 65°C	When the chassis inlet temperature is less than 50°C, or when the chassis outlet temperature is less than 65°C
Major	Chassis temperature too low	When the chassis inlet temperature is less than or equal to –40°C, or when the chassis outlet temperature is less than or equal to –40°C	When the chassis inlet temperature is greater than –40°C, or when the chassis outlet temperature is greater than –40°C
Major	Temperature rating mismatch	When a chassis contains at least one industrial temperature component and at least one commercial temperature component	When all components in a chassis are industrial temperature, or when all components in a chassis are commercial temperature
Major	Door open alarm	Alarm generated by equipment wired to connector P4 pin 0 on the I/O card	Alarm cleared by equipment wired to connector P4 pin 0 on the I/O card
Major	Station alarm 1	Alarm generated by equipment wired to connector P5 pin 1 on the I/O card	Alarm cleared by equipment wired to connector P5 pin 1 on the I/O card
Major	Station alarm 2	Alarm generated by equipment wired to connector P5 pin 3 on the I/O card	Alarm cleared by equipment wired to connector P5 pin 3 on the I/O card
Major	Station alarm 3	Alarm generated by equipment wired to connector P5 pin 2 on the I/O card	Alarm cleared by equipment wired to connector P5 pin 2 on the I/O card
Major	Fan Slot not detected or missing	When the agent does not detect the presence of a fan tray in the corresponding fan tray slot	When the agent detects the presence of a fan tray in the corresponding fan tray slot
Major	Input voltage out of range	When the input voltage is less than minimum (VAC) or when the input voltage is greater than maximum (VAC)	When the input voltage is greater than or equal to minimum (VAC) and less than or equal to maximum (VAC)
Major	Excessive current	When the product of the input voltage and input current is greater than 1050 W	When the product of the input voltage and the input current is less than or equal to 1050 W
Major	Fan voltage out of range	When the fan voltage is less than minimum VDC or when the fan voltage is greater than maximum VDC	When the fan voltage is greater than or equal to minimum VDC and less than or equal to maximum VDC
Major	Power supply fault	When the power supply indicates a fault	When the power supply does not indicate a fault
Major	Temperature exceeds limit	When the internal power supply temperature is greater than or equal to 50°C, or when the external power supply temperature is greater than or equal to 65°C	When the internal power supply temperature is less than 50°C and the external power supply temperature is less than 65°C

Table A-7 Cisco 6260 Alarms (continued)

Alarm Severity	Description	Asserted	Cleared
Minor	Single fan failure	When a single fan contained by the fan tray has failed	When all fans contained by the fan tray are functioning properly or when more than one fan contained by the fan tray has failed
Major	Multiple fan failures	When more than one fan contained by the fan tray has failed	When all fans contained by the fan tray are functioning properly or when a single fan contained by the fan tray has failed
Minor	Fan tray not detected or missing	When the agent does not detect the presence of a fan tray in the corresponding power supply bay	When the agent detects the presence of a fan tray in the corresponding power supply bay

ADSL-CAP Alarms

Table A-8 describes alarms specific to ADSL-CAP cards.

Table A-8 ADSL-CAP Alarms

Alarm Severity	Description	Asserted	Cleared
Minor	SNR margin below config value	When the actual SNR margin is less than the SNR margin threshold	When the actual SNR margin is greater than or equal to the SNR margin threshold
Minor	Upstream rate below minimum rate	When the actual upstream rate is less than the provisioned minimum upstream rate	When the actual upstream rate is greater than or equal to the provisioned minimum upstream rate
Minor	Downstream rate below minimum rate	When the actual downstream rate is less than the provisioned minimum downstream rate	When the actual downstream rate is greater than or equal to the provisioned minimum downstream rate
Minor	CPE signature below config value	When the actual CPE signature is less than the provisioned CPE signature	When the actual CPE signature is greater than or equal to the provisioned CPE signature
Minor	LOS, LOF, or LOCD failure	When the ADSL CAP line interface experiences one of the following defects: LOS, LOF, LOCD	When the ADSL CAP line interface experiences none of the following defects: LOS, LOF, LOCD

ADSL-DMT Alarms

Table A-9 describes alarms specific to ADSL-DMT cards.

Table A-9 ADSL-DMT Alarms

Alarm Severity	Description	Asserted	Cleared
Minor	ATU-C port failure	When the ATU-C can not communicate with the chip set implementing the port	When the ATU-C can communicate with the chip set implementing the port
Minor	Upstream rate below minimum rate	When the interleaved channel's actual upstream rate is less than the provisioned minimum upstream rate or when the fast channel's actual upstream rate is less than the provisioned minimum upstream rate	When the both the interleaved channel's actual upstream rate is greater than or equal to the provisioned minimum upstream rate, and the fast channel's actual upstream rate is greater than or equal to the provisioned minimum upstream rate
Minor	Downstream rate below minimum rate	When the interleaved channel's actual downstream rate is less than the provisioned minimum downstream rate or when the fast channel's actual downstream rate is less than the provisioned minimum downstream rate	When the both the interleaved channel's actual downstream rate is greater than or equal to the provisioned minimum downstream rate, and the fast channel's actual downstream rate is greater than or equal to the provisioned minimum downstream rate
Minor	LOS, LOF, LOCD or LPR failure	When the ADSL DMT line interface experiences one of the following defects: LOS, LOF, LOCD, or far-end LPR	When the ADSL DMT line interface experiences none of the following defects: LOS, LOF, LOCD, or far-end LPR

SDSL Alarms

Table A-10 describes alarms specific to SDSL cards.

Table A-10 SDSL Alarms

Alarm Severity	Description	Asserted	Cleared
Minor	STUC port failure	When the line is configured to be administratively up, but it is operationally down; in other words, there is no physical layer connectivity with the CPE	When the line has physical layer connectivity with the CPE Or when the line is administratively down
Minor	SNR margin below config value	When the actual SNR margin is less than the SNR margin threshold	When the actual SNR margin is greater than or equal to the SNR margin threshold
Minor	Bit rate below minimum rate	When the actual rate is less than the provisioned minimum rate	When the actual rate is greater than or equal to the provisioned minimum rate

G. SHDSL Alarms

Table A-11 describes alarms specific to G.SHDSL cards.

Table A-11 SHDSL Alarms

Alarm Severity	Description	Asserted	Cleared
Minor	STUC port failure	When the line is configured to be administratively up, but it is operationally down; in other words, when there is no physical layer connectivity with the CPE	When the line has physical layer connectivity with the CPE or when the line is administratively down
Minor	SNR margin below config value	When the actual SNR margin is less than the SNR margin threshold	When the actual SNR margin is greater than or equal to the SNR margin threshold
Minor	Bit rate below minimum rate	When the actual rate is less than the provisioned minimum rate.	When the actual rate is greater than or equal to the provisioned minimum rate.
Minor	Oversubscription	When the total provisioned bit rates on odd or even ports are less than 5 Mbps.	When the total provisioned bit rates on odd or even ports are greater than or equal to 5 Mbps

DS3/DS3 NI-2 Alarms

Table A-12 describes alarms specific to DS3/DS3 NI-2 configurations.

Table A-12 Alarms Specific to DS3/DS3 NI2 Configurations

Alarm Severity	Description	Asserted	Cleared
Critical	RAI Received	When the DS3 interface experiences an RAI defect	When the DS3 interface is not experiencing an RAI defect
Critical	Yellow Alarm Received	When the DS3 interface experiences a yellow alarm	When the DS3 interface is not experiencing a yellow alarm
Critical	AIS Received	When the DS3 interface experiences an AIS defect	When the DS3 interface is not experiencing an AIS defect
Critical	OOF Received	When the DS3 interface experiences an OOF defect	When the DS3 interface is not experiencing an OOF defect
Critical	LOS Detected	When the DS3 interface experiences an LOS defect	When the DS3 interface is not experiencing an LOS defect
Critical	PLCP LOF Detected	When the DS3 interface experiences a PLCP LOF defect	When the DS3 interface is not experiencing a PLCP LOF defect
Critical	FERF Received	When the DS3 interface experiences an FERF defect	When the DS3 interface is not experiencing an FERF defect
Critical	FEBE Received	When the DS3 interface experiences an FEBE defect	When the DS3 interface is not experiencing an FEBE defect
Critical	RAI Received	When the DS3 interface experiences an RAI defect	When the DS3 interface is not experiencing an RAI defect

Table A-12 Alarms Specific to DS3/DS3 NI2 Configurations (continued)

Alarm Severity	Description	Asserted	Cleared
Critical	Yellow Alarm Received	When the DS3 interface experiences a yellow alarm	When the DS3 interface is not experiencing a yellow alarm
Critical	AIS Received	When the DS3 interface experiences an AIS defect	When the DS3 interface is not experiencing an AIS defect
Critical	OOF Received	When the DS3 interface experiences an OOF defect	When the DS3 interface is not experiencing an OOF defect
Critical	LOS Detected	When the DS3 interface experiences an LOS defect	When the DS3 interface is not experiencing an LOS defect
Critical	PLCP LOF Detected	When the DS3 interface experiences an PLCP LOF defect	When the DS3 interface is not experiencing an PLCP LOF defect
Critical	Subtend Port Configured as Trunk	Subtend port configured as trunk	Subtend port not configured as trunk

DS3/T1E1 NI-2 Alarms

Table A-13 describes alarms specific to DS3/T1E1 NI-2 configurations.

Table A-13 Alarms Specific to DS3/T1E1 NI2 Configurations

Alarm Severity	Description	Asserted	Cleared
Critical	Loss of Cell Delineation	When the DS3 interface experiences an LOCD defect	When the DS3 interface is not experiencing an LOCD defect
Critical	Loss of Cell Delineation	When the DS3 interface experiences an LOCD defect	When the DS3 interface is not experiencing an LOCD defect

E1 IMA Group Alarms

Table A-14 describes alarms specific to E1 IMA groups.

Table A-14 E1 IMA Group Alarms

Alarm Severity	Description	Asserted	Cleared
Critical	Configuration Abort	When the FE tries to use unacceptable configuration parameters	When the FE tries to use acceptable configuration parameters
Critical	Configuration Abort - FE	When the FE reports unacceptable configuration parameters	When the FE reports acceptable configuration parameters
Critical	Insufficient Links	When less than P(Tx) transmit or P(Rx) receive links are active	When at least P(Tx) transmit or P(Rx) receive links are active
Critical	Insufficient Links - FE	When the FE reports that fewer than P(Tx) transmit or P(Rx) receive links are active	When the FE reports that at least P(Tx) transmit or P(Rx) receive links are active

Table A-14 E1 IMA Group Alarms (continued)

Alarm Severity	Description	Asserted	Cleared
Critical	Blocked - FE	When the FE reports that it is blocked	When the FE reports that it is not blocked
Critical	Timing Mismatch	When the FE transmit clock mode is different from the NE transmit clock mode	When the FE transmit clock mode is the same as the NE transmit clock mode

E1 IMA Link Alarms

Table A-15 describes alarms specific to E1 IMA Links.

Table A-15 E1 IMA Link Alarms

Alarm Severity	Description	Asserted	Cleared
Critical	Alarm Indication Signal	When the IMA interface experiences an AIS defect	When the IMA interface is not experiencing an AIS defect
Critical	Remote Alarm Indication	When the IMA interface experiences an RAI defect	When the IMA interface is not experiencing a RAI defect
Critical	Loss of Cell Delineation	When the IMA interface experiences an LOCD defect	When the IMA interface is not experiencing an LOCD defect
Critical	Loss of IMA Frame	Persistence of a LIF defect at the NE	No persistence of an LIF defect at the NE
Critical	Link Out of Delay Sync	Persistence of a LODS defect at the NE	No persistence of an LODS defect at the NE
Critical	Tx Link Misconnected	When the Tx link is detected as misconnected. This is reported when the IMA unit has determined that the Tx link is not connected to the same FE IMA unit as the other Tx links in the group. The detection is implementation-specific.	When the Tx link is not detected as misconnected
Critical	Rx Link Misconnected	When the Rx link is detected as misconnected. This is reported when the IMA unit has determined that the Rx link is not connected to the same FE IMA unit as the other Rx links in the group. The detection is implementation-specific.	When the Rx link is not detected as misconnected
Critical	Rx Fault	Implementation-specific Rx fault declared at the NE	Implementation specific Rx fault not declared at the NE
Critical	Tx Fault	Implementation-specific Tx fault declared at the NE	Implementation specific Tx fault not declared at the NE
Critical	Tx Link Unusable - FE	When the FE reports Tx-Unusable	When the FE does not report Tx-Unusable
Critical	Rx Link Unusable - FE	When the FE reports Rx-Unusable	When the FE does not report Rx-Unusable

T1 IMA Group Alarms

Table A-16 describes alarms specific to T1 IMA Groups.

Table A-16 T1 IMA Group Alarms

Alarm Severity	Description	Asserted	Cleared
Critical	Configuration Abort	When the FE tries to use unacceptable configuration parameters	When the FE tries to use acceptable configuration parameters
Critical	Configuration Abort - FE	When the FE reports unacceptable configuration parameters	When the FE reports acceptable configuration parameters
Critical	Insufficient Links	When less than P(Tx) transmit or P(Rx) receive links are Active	When at least P(Tx) transmit or P(Rx) receive links are Active
Critical	Insufficient Links - FE	When the FE reports that less than P(Tx) transmit or P(Rx) receive links are active	When the FE reports that at least P(Tx) transmit or P(Rx) receive links are active
Critical	Blocked - FE	When the FE reports that it is blocked	When the FE reports that it is not blocked
Critical	Timing Mismatch	When the FE transmit clock mode is different than the NE transmit clock mode	When the FE transmit clock mode is the same as the NE transmit clock mode

T1 IMA Link Alarms

Table A-17 describes alarms specific to T1 IMA Links.

Table A-17 T1 IMA Link Alarms

Alarm Severity	Description	Asserted	Cleared
Critical	Alarm Indication Signal	When the IMA interface experiences an AIS defect	When the IMA interface is not experiencing an AIS defect
Critical	Remote Alarm Indication	When the IMA interface experiences an RAI defect	When the IMA interface is not experiencing an RAI defect
Critical	Loss of Cell Delineation	When the IMA interface experiences an LOCD defect	When the IMA interface is not experiencing an LOCD defect
Critical	Loss of IMA Frame	Persistence of an LIF defect at the NE	No persistence of an LIF defect at the NE
Critical	Link Out of Delay Sync	Persistence of an LODS defect at the NE	No persistence of an LODS defect at the NE
Critical	Tx Link Misconnected	When the Tx link is detected as mis-connected. This is reported when the IMA unit has determined that the Tx link is not connected to the same FE IMA unit as the other Tx links in the group. The detection is implementation-specific.	When the Tx link is not detected as misconnected

Table A-17 T1 IMA Link Alarms (continued)

Alarm Severity	Description	Asserted	Cleared
Critical	Rx Link Misconnected	When the Rx link is detected as misconnected. This is reported when the IMA unit has determined that the Rx link is not connected to the same FE IMA unit as the other Rx links in the group. The detection is implementation-specific.	When the Rx link is not detected as misconnected
Critical	Rx Fault	Implementation-specific Rx fault declared at the NE	Implementation specific Rx fault not declared at the NE
Critical	Tx Fault	Implementation-specific Tx fault declared at the NE	Implementation specific Tx fault not declared at the NE
Critical	Tx Link Unusable - FE	When the FE reports Tx-Unusable	When the FE does not report Tx-Unusable
Critical	Rx Link Unusable - FE	When the FE reports Rx-Unusable	When the FE does not report Rx-Unusable

OC-3 Alarms

Table A-18 describes alarms specific to OC-3 cards.

Table A-18 OC3 Alarms

Alarm Severity	Description	Asserted	Cleared
Critical	Loss of Cell Delineation	When the ATM interface associated with the SONET/SDH interface experiences an LOCD defect	When the ATM interface associated with the SONET/SDH interface is not experiencing LOCD defect
Minor	Signal Label Mismatch	When the SONET/SDH path experiences a signal mismatch defect	When the SONET/SDH path is not experiencing a signal mismatch defect
Critical	Path RDI Received	When the SONET/SDH path experiences a RDI defect	When the SONET/SDH path is not experiencing an RDI defect
Critical	Path AIS Received	When the SONET/SDH path experiences an AIS defect	When the SONET/SDH path is not experiencing an AIS defect
Critical	Loss of Pointer	When the SONET/SDH path experiences an LOP defect	When the SONET/SDH path is not experiencing an LOP defect
Critical	Line RDI	When the SONET/SDH line experiences an RDI defect	When the SONET/SDH line is not experiencing an RDI defect
Critical	Line AIS Received	When the SONET/SDH line experiences an AIS defect	When the SONET/SDH line is not experiencing an AIS defect
Critical	Loss of Frame	When the SONET/SDH section experiences an LOF defect	When the SONET/SDH section is not experiencing an LOF defect
Critical	Loss of Signal	When the SONET/SDH section experiences an LOS defect	When the SONET/SDH section is not experiencing an LOS defect

Miscellaneous Alarms

Table A-19 describes miscellaneous alarms.

Table A-19 Miscellaneous Alarms

Description	Asserted	Cleared
Major	Loss of active clock sync	When the network clock contains the BITS clock in its priority list and the BITS clock exhibits an LOS or an AIS
Major	BITS clock failure	When the current clock source of the network clock is priority 5
Major	Active/Standby NI2 type mismatch	When active and standby NI2 cards are mismatched
Major	Standby NI2 missing	When the standby card is missing
Minor	Module not equal to provisioning	When the agent detects the presence of a module that has a vendor type that does not match the provisioning for the slot
Major	Provisioned slot is empty	When the agent does not detect a module in a provisioned slot, that is, when the module is removed
Minor	Invalid module for this slot	When the agent detects the presence of an unsupported (or unrecognized) module
Info	Module was detected	When the agent detects the presence of a supported module, that is, when the module is inserted
Info	Flex module not provisioned	When a Flex module is not provisioned as either DMT or CAP
MAJOR	Loss of active clock sync	When the network clock contains the BITS clock in its priority list and the BITS clock exhibits an LOS or an AIS
MAJOR	BITS clock failure	When the current clock source of the network clock is priority 5

Creating User Groups and Using the Technology-Specific Commands

This appendix includes information and instructions for creating user groups through the Cisco EMF Groups application and for using the technology-specific commands from the Tools menu.

This appendix includes the following sections:

- Creating User Groups, page B-1
- Using the Technology Commands and Tools, page B-10

Creating User Groups

You can customize user access to certain software functions by using the Cisco EMF user access control feature. Access to features can be restricted on the basis of user access level to a subset, or group, of these features. For example, users for a particular site or region in which a site belongs should administer objects that are within that site.

Accessibility includes the following four levels of user access:

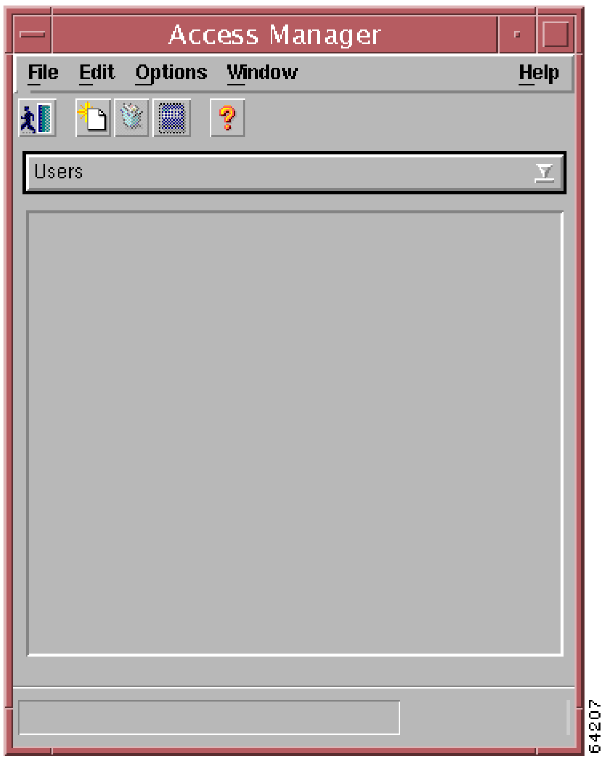
- Technical support (T)
- Provisioning (P)
- Operations (O)
- Network management (N)

Creating User Groups

To create a user group, complete the following steps:

Step 1 Click the **Access** icon on the Cisco EMF Launchpad window to open the Access Manager window. (See Figure B-1.)

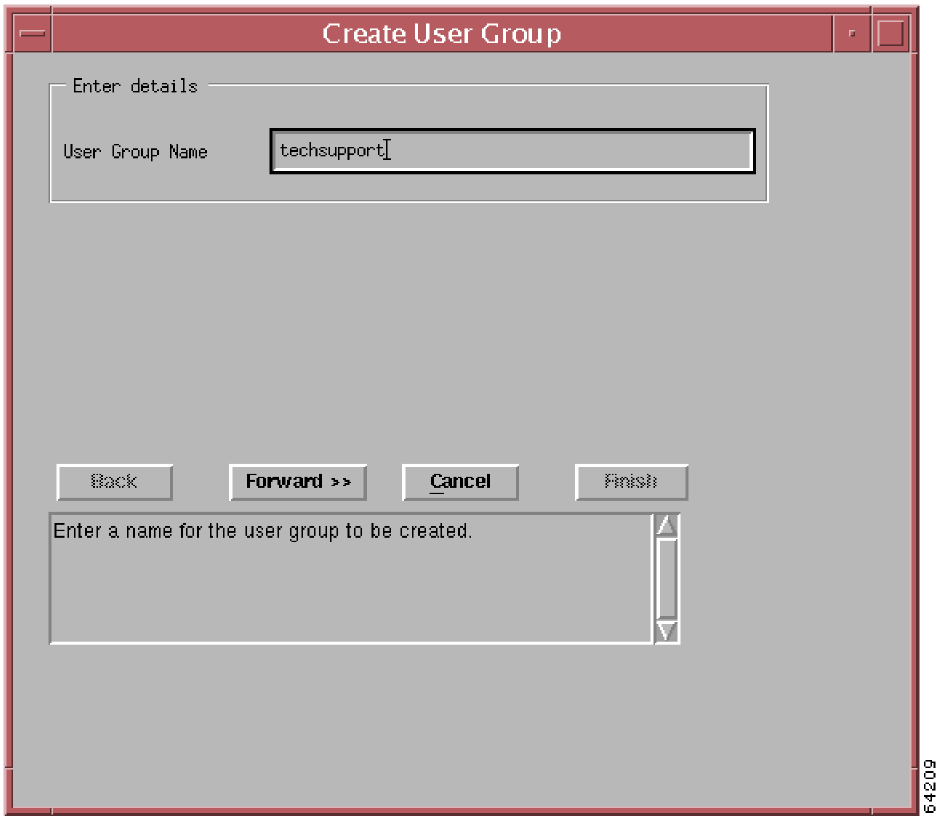
Figure B-1 Access Manager Window



Step 2 Choose **Create > User Group** from the Edit menu.

The Create User Group window opens. (See Figure B-2.)

Figure B-2 Create User Group Window

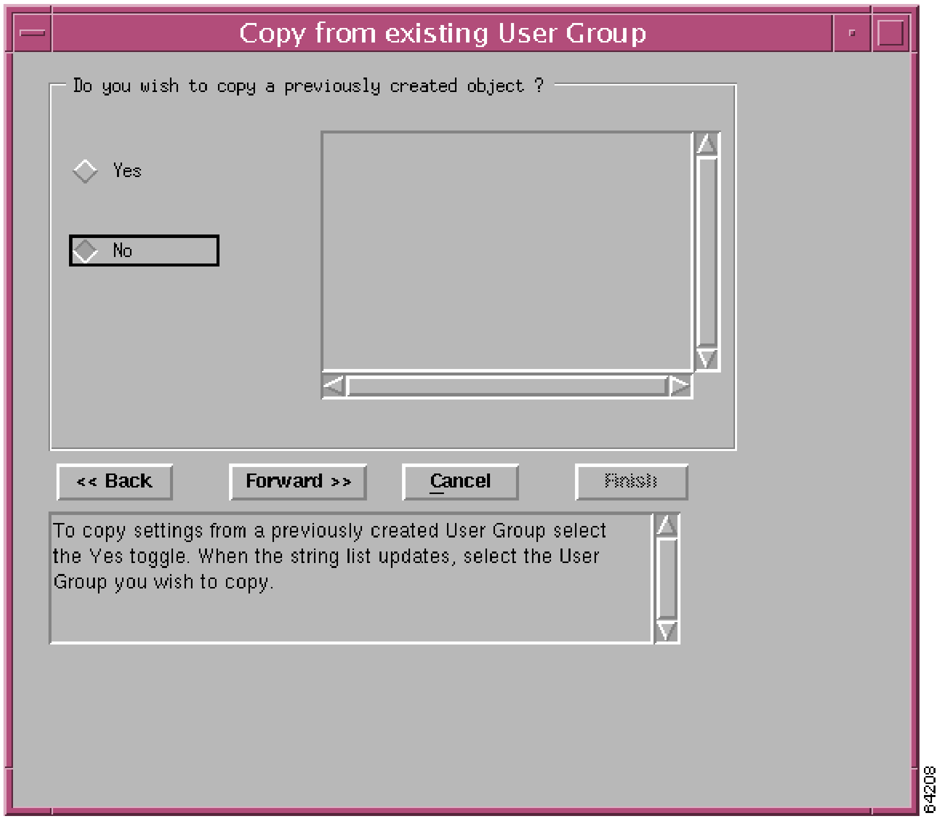


Step 3 In the User Group Name field, enter the name of the user group that you want to create, for example, techsupport.

Step 4 Click **Forward**.

The Copy from Existing User Group window opens. (See Figure B-3.)

Figure B-3 Copy from Existing User Group Window



If you want to use the specifications of a current group, you can click **Yes** and choose a group whose specifications you want to copy.

Step 5 If you are creating a new, customized user group, click **No**, and then click **Forward**.

The Select Users window opens.

Note An administrator will have already set up the users on the system for which you are creating a user group.

Step 6 In the Available Users column on the left side of the window, highlight the names of the users that you want to include in this user group.

Step 7 Click the right-pointing arrow to move the name of that user to the Selected Users column on the right.

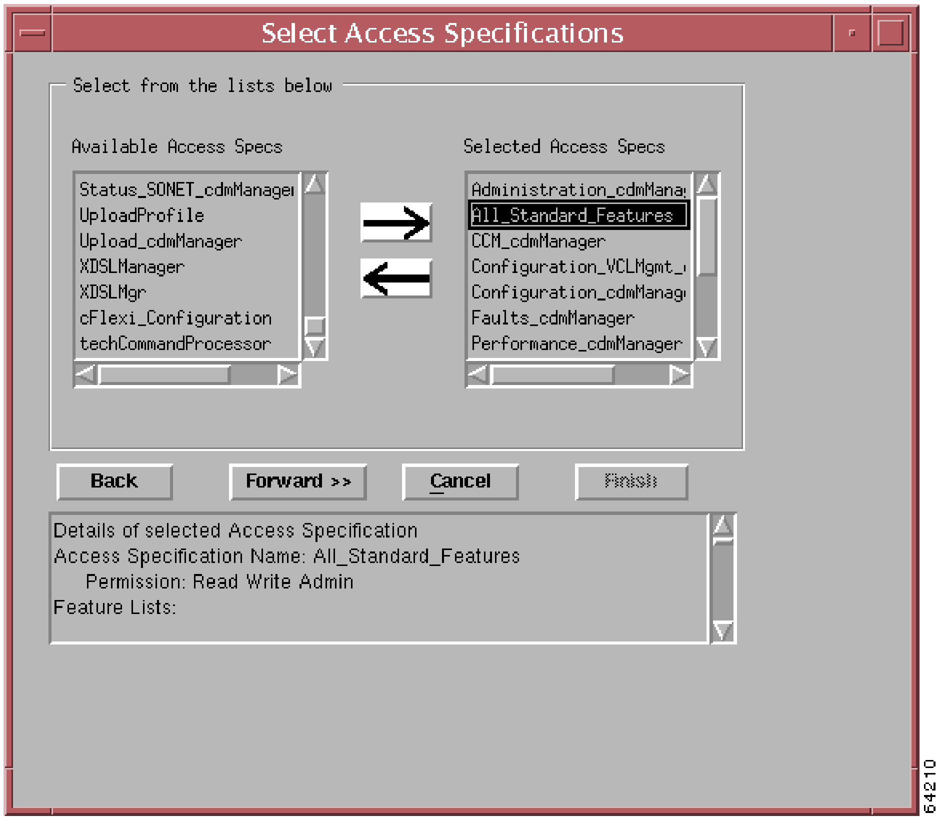
Step 8 Repeat Step 7 for each user that you want to add to the Selected Users column.

Step 9 Click the left-pointing arrow to move a user from the Selected Users column back to the Available Users column if you do not want that user to be a part of the group you are creating.

Step 10 Click **Forward**.

The Select Access Specification window opens. (See Figure B-4.)

Figure B-4 Select Access Specification Window



Step 11 Highlight the specifications that you want to include in this user group from the Available Access Specifications list on the left side of the window.

Step 12 Click the right-pointing arrow to move the name of that specification to the Selected Access Specifications column on the right.

> **Note** See the "Access Specifications for the User Groups" section on page B-7 for more detailed information about the access specifications for each type of user group that is available in CDM.

Step 13 Repeat Step 11 for each specification that you want to add to the Selected Access Specifications column.

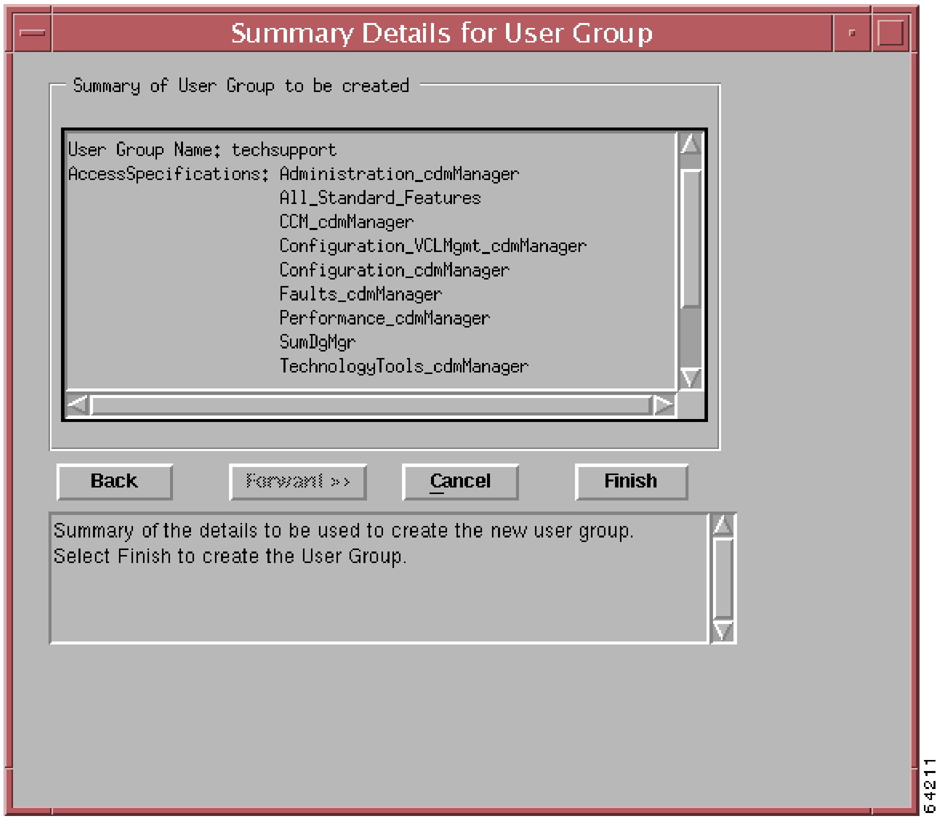
> **Note** For all groups, be sure that you click All_Standard_Features in the Available Access Specifications column on the Select Access Specifications window.

Step 14 Click the left-pointing arrow to move a user from the Selected Access Specifications column back to the Available Access Specifications column if you do not want that specification to be a part of the user group definition.

Step 15 Click **Forward**.

The Summary Details for User Group window opens. (See Figure B-5.)

Figure B-5 Summary Details for User Group



This window displays the following information about the group that you have created (with examples):

- User Group Name: techsupportexample
- Users: techsupport
- Access Specification: ADSL_Configuration

Step 16 Click **Finish** to complete the creation of the user group.

Access Specifications for the User Groups

The following sections list the specifications for each of the four user groups. Table B-1 provides an overview of each specification and its purpose, and it indicates the user group in which the specification is included.

Table B-1 Access Specifications for User Groups

Access Specification	Purpose/Service	Technical Support	Provisioning	Operations	Network Management
Administration_cdmManager	IOS password, SNMP, Backup/Restore windows	x			x
All_Standard_Features	Basic Cisco EMF functionality	x	x	x	x
CCM_cdmManager	Cross connection management	x	x		
cdmManager	Deploy DSLAM	x			
cFlexi_Configuration	Flexi card configuration	x			
Configuration_cdmManager	Generic configuration windows	x	x		
Configuration_E3_cdmManager	E3/DS3 configuration windows	x			
Configuration_VCLMgmt_ cdmManager	VCL management configuration	x			
Deploy_FrAtmCM	Deploy FR/ATM connection	x			
Deploy_PPPoACM	Deploy PPP connection	x			
DMT_Status		x		x	
Faults_cdmManager	Fault Management windows	x	x	x	
FrAtmCM		x			
Performance_ADSL	ADSL Performance	x			
Performance_cdmManager	Generic Performance windows	x			
Performance_VCLMgmt_cdmManager	VCL management performance	x			
Profile_XDSLMgr	XDSL Interface Manager window	x	x		
QoS_cdmManager	Quality of Service windows	x			
Status_ADSL(Status)		x	x	x	
Status_DMT_cdmManager	DMT Inventory Status	x	x		

Table B-1 Access Specifications for User Groups (continued)

Access Specification	Purpose/Service	Technical Support	Provisioning	Operations	Network Management
StatusInvSum_ISSMgr	Status and Inventory windows	x	x	x	
StatInvSumm_cdmManager	Status and Inventory windows	x	x	x	
subtendManager	Subtend Manager windows	x			
SumDgMgr	Chassis Summary windows	x	x	x	
techCommandProcessor	Technology-specific commands	x	x	x	
TechnologyTools_cdmManager	Telnet commands	x	x	x	
Upload_cdmManager	Upload Profile windows	x			
ViewLogs_cdmManager	Syslog and Event Command windows	x	x	x	x

The following sections list the access specifications for each group.

Technical Support Group (T)

The technical support (T) group should contain the following access specifications:

- Administration_cdmManager
- All_Standard_Features
- CCM_cdmManager
- cdmManager
- cFlexi_Configuration
- Configuration_cdmManager
- Configuration_E3_cdmManager
- Configuration_VCLMgmt_cdmManager
- Deploy_FrAtmCM
- Deploy_PPPoACM
- DMT_Status
- Faults_cdmManager
- FrAtmCM
- Performance_ADSL(Performance)
- Performance_cdmManager
- Performance_VCLMgmt_cdmManager
- Profile_XDSLMgr
- QOS_cdmManager

- StatInvSum_cdmManager
- Status_ADSL(Status)
- Status_DMT_cdmManager
- StatusInvSum_ISSSMgr
- subtendManager
- SumDgMgr
- techCommandProcessor
- TechnologyTools_cdmManager
- Upload_cdmManager
- ViewLogs_cdmManager

Provisioning Group (P)

The provisioning (P) group should contain the following access specifications:

- All_Standard_Features
- CCM_cdmManager
- Configuration_cdmManager
- Faults
- Profile_cdmManager
- Profile_XDSLMgr
- QoS_cdmManager
- StatInvSumm_cdmManager
- Status_ADSL(Status)
- Status_DMT_cdmManager
- StatusInvSum_ISSMgr
- SumDgMgr
- techCommandProcessor
- TechnologyTools_cdmManager
- ViewLogs_cdmManger

Operations Group (O)

The operations (O) group should contain the following access specifications:

- All_Standard_Features
- DMT_Status
- Faults_cdmManager
- Status_ADSL(Status)
- StatInvSum_cdmManager
- StatusInvSum_ISSMgr
- SumDgMgr

- techCommandProcessor
- TechnologyTools_cdmManager
- ViewLogs_cdmManager

Network Management Group (N)

The network management (N) group should contain the following access specifications:

- Administration_cdmManager
- All_Standard_Features
- ViewLogs_cdmManager

Using the Technology Commands and Tools

This section describes how to invoke certain IOS commands and initiate a Telnet session from the object menu. The IOS commands are executed by using Telnet sessions to the node. You can access the technology commands from the chassis, module (or line card), and interface levels. The choices that display depend on the type of object you click to access the menu and include:

- Save Running Config (chassis)
- Check Alarms on the Chassis (chassis)
- Set Chassis Temperature-rating as Commercial (chassis)—sets the temperature for commercial Cisco 6015 DSLAMs
- Set Chassis Temperature-rating as OSP (chassis)—sets the temperature for Cisco 6015 DSLAMS that are specified as outside plant
- Check Chassis Temperature Status (chassis)
- Show run int atm (interface)
- Show dsl int atm (interface)
- Show atm vc traffic int atm (interface, PVC, and SPVC objects)
- Show atm vc int atm (interface)
- reset card (module, or line card)
- Clear ATM int (interface)
- Shut (interface)
- No Shut (interface)

The Technology Tools menu item contains one choice, Telnet, which opens a telnet window.

Invoking IOS Commands Using the Technology-Specific Commands Menu Choices

Complete the following steps to invoke the IOS commands:

Step 1 Right-click the icon for an object on the left side of the Map Viewer window from the Component Managed view or the Physical view.

Step 2 Choose **Cisco DSL Manager > Technology Commands**.

The Technology Commands menu displays. Examples of the menus are shown in Figure B-6, Figure B-7, and Figure B-8.

Figure B-6 Example of Chassis Technology Commands Menu

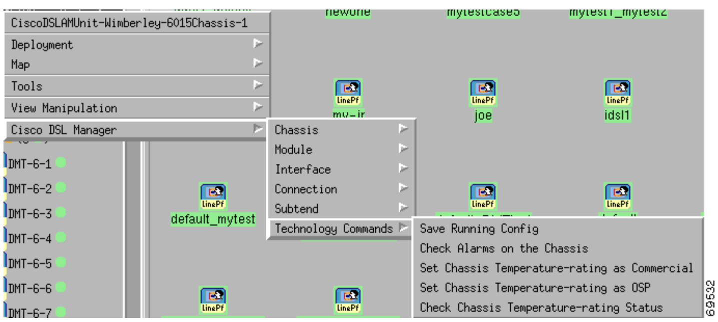


Figure B-7 Example of Interface Technology Commands Menu

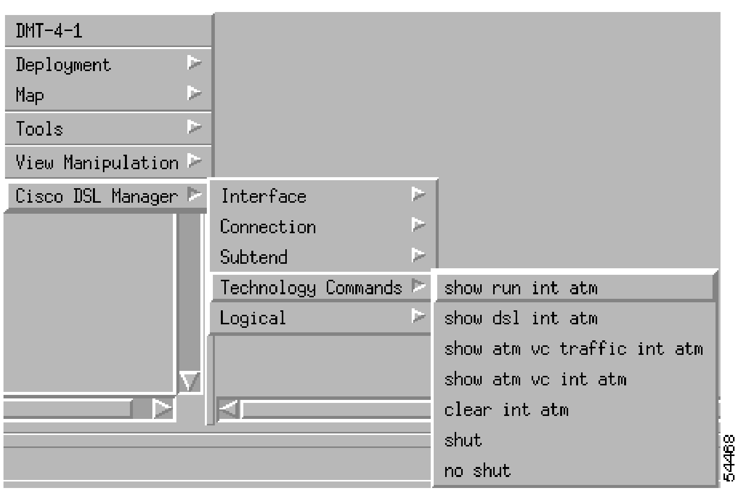
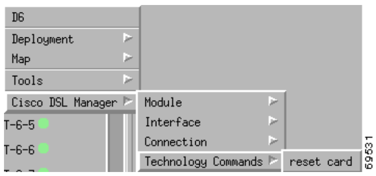


Figure B-8 Example of Line Card Technology Commands Menu

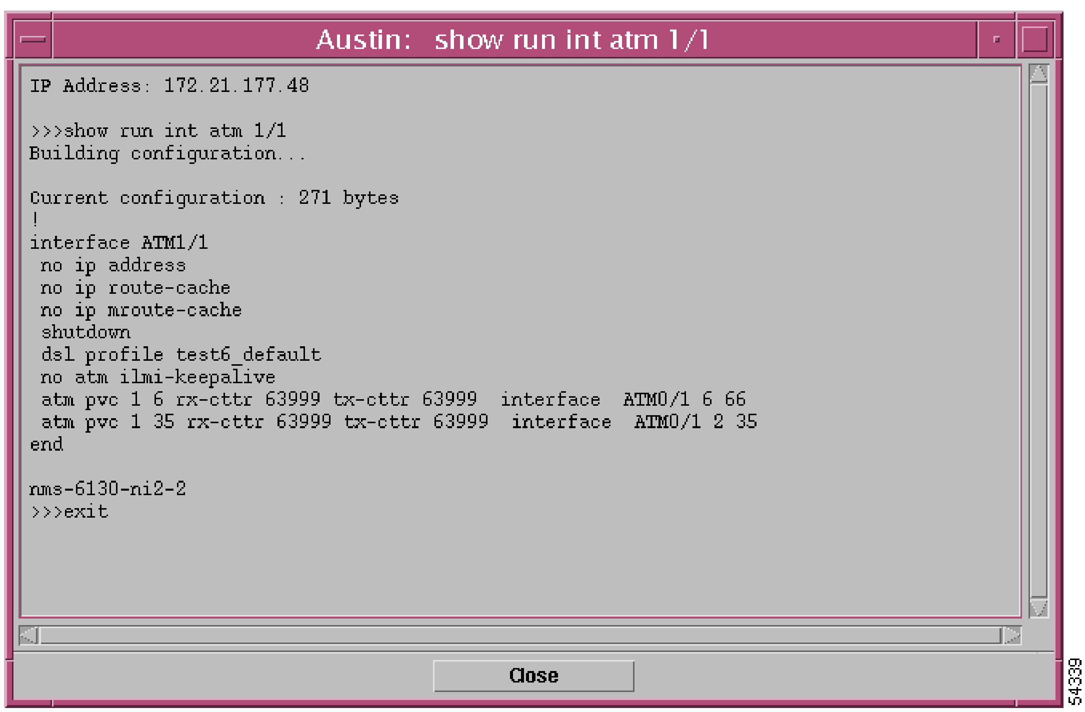


Step 3 Place your cursor over Technology Commands on the object menu and choose from the options that display.

The menu that displays depends on whether you place your cursor over a DSLAM (chassis), an interface, or a line card. Figure B-6 shows an example of an object menu that opens when you access this menu from a module. Table B-2 describes the menu choices.

A CLI output window opens when you choose an item from the Technology Specific Commands menu. The name of the window that opens corresponds to the name of the DSLAM, the menu item that you choose, and the related module and slot numbers. An example of the CLI output window is shown in Figure B-9.

Figure B-9 Example of a CLI Output WIndow



In Figure B-9, the window that opens is a result of placing your cursor over a module and choosing Technology Specific Commands > show run int atm. The 1/1 in the window title refers to module 1 slot 1.

Table B-2 describes the Technology Specific Commands menu choices, which open a telnet window and issue an IOS command to the IP address of the associated DSLAM.

Table B-2 Technology Specific Commands

Command	Description	Restrictions
Chassis Technology Commands		
Save Running Config	Choose this item from a DSLAM (chassis object) to issue the Save Running Config command and manually sync up the IOS running configuration or the IOS startup configuration. **Note** After you apply a DSL profile, you need to use the Save Running Config option to sync up the two configurations. This process is different from that used in earlier CDM releases.	None
Check Alarms on the Chassis	Choose this item from a DSLAM (chassis object) to issue the show facility-alarm status command and transfer the IOS login user name and login password.	None
Set Chassis Temperature-rating as Commercial	Choose this item from a DSLAM (chassis object) to issue the set temperature rating command to for commercial Cisco 6015 DSLAMs. This is the default. A temperature rating mismatch alarm is triggered when any installed system component has a different temperature rating than the system temperature rating setting.	Commercial Cisco 6015 DSLAMs only.
Set Chassis Temperature-rating as OSP	Choose this item from a DSLAM (chassis object) to issue the set temperature rating command for outside plant environment (OSP) Cisco 6015 DSLAMs.	OSP Cisco 6015 DSLAMs only.
Check Chassis Temperature-rating Status	Choose this item from a DSLAM (chassis object) to issue the show environment command and display information about system temperature settings.	
Interface Technology Commands		
show run int[1] atm	Choose this item from an interface object (line card) to issue the show run int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.	None
show dsl int atm	Choose this item from an interface object (line card) to issue the show dsl int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.	None
show atm vc traffic int atm	Choose this item from an interface object (line card), PVC, or SPVC object to issue the show atm vc traffic int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.	None
show atm vc int atm	Choose this item from an interface object (line card) to issue the show atm vc int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.	None

Table B-2 Technology Specific Commands (continued)

Command	Description	Restrictions
clear atm int	Choose this item from an interface object (line card) to issue the clear ATM int command and transfer the login user name, login password, slot number, and port number.	Only DSL line cards support this command.
shut	Choose this item from an interface object (line card) to issue the shut int atm command and transfer the login user name, login password, slot number, and port number.	Only DSL line cards support this command.
no shut	Choose this item from an interface object (line card) to issue the no shut int atm command and transfer the login user name, login password, slot number, and port number.	Only DSL line cards support this command.
Module or Line Card Technology Command		
reset card	Choose this item from a module to open the CLI Reset Card window and transfer the IOS login user name, login password, and enable password.	Only DSL line cards support this command.

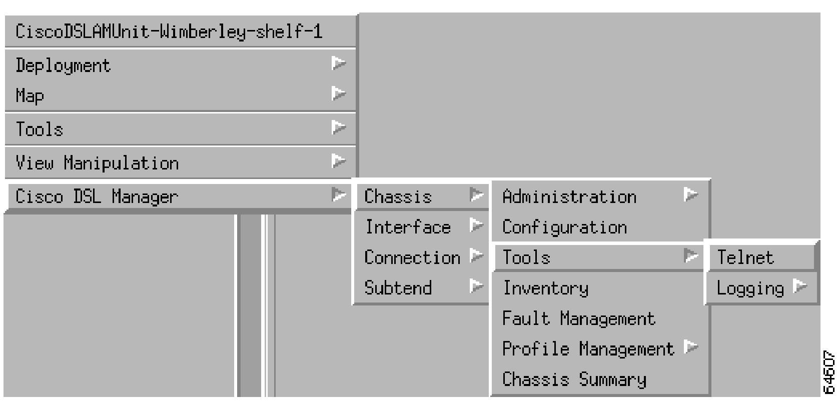
1. int = interface

Opening a Telnet Session to the DSLAM

To open a Telnet session from the CDM GUI, complete the following steps:

Step 1 From the left side of the Map Viewer window within any view, right-click the chassis to access the object menu opens. (See Figure B-10.)

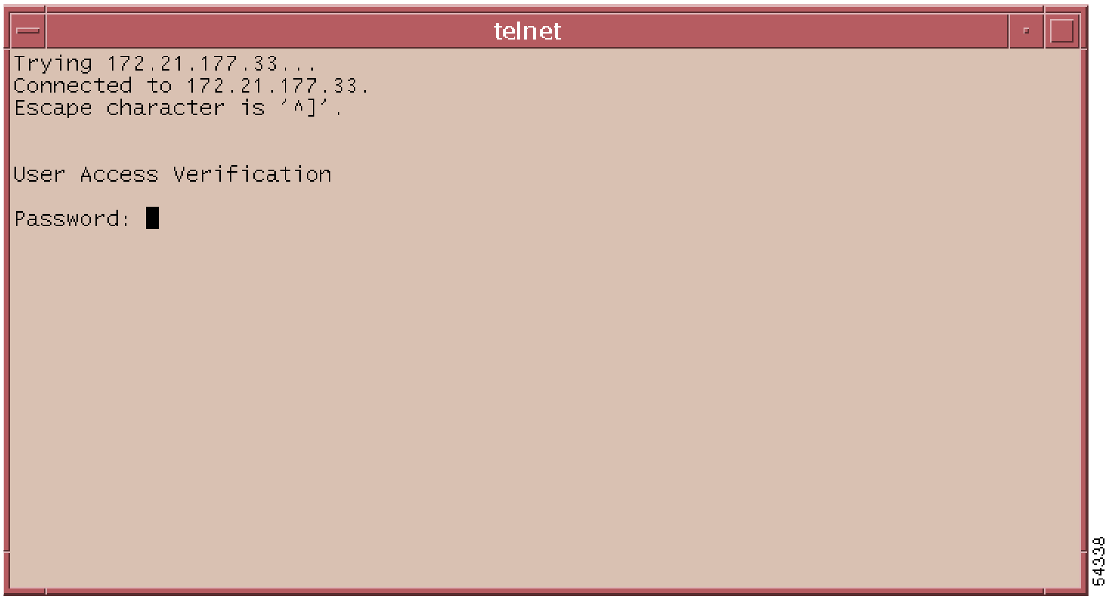
Figure B-10 Chassis Tools Menu



Step 2 Choose **Cisco DSL Manager > Chassis > Tools > Telnet** to open the Telnet window.

Figure B-11 shows an example of a Telnet window.

Figure B-11 Example of a Telnet Window



APPENDIX C

Using the Cisco DSL Manager Object Menus

This appendix provides detailed descriptions of the object menus that you can access from the Cisco DSL Manager menu.

This appendix includes the following sections:

- Overview of the Cisco DSL Manager Object Menus, page C-1
- Summary of Cisco DSL Manager Object Menus, page C-6

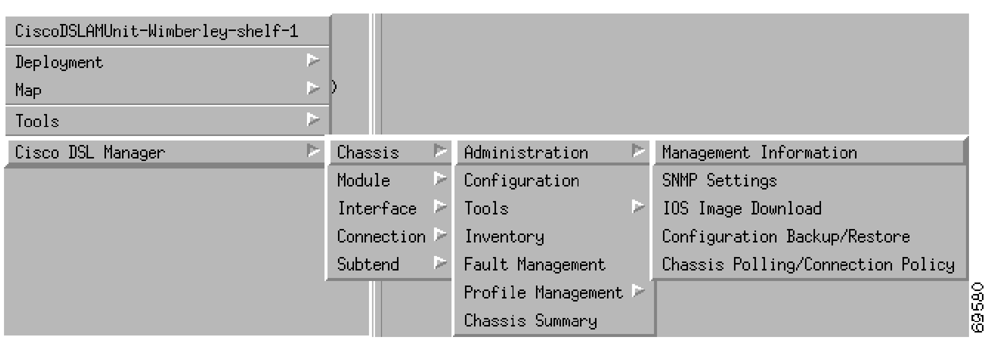
Overview of the Cisco DSL Manager Object Menus

To access most of the windows through which you manage the Cisco DSLAM, you use the Cisco DSL Manager menu. This menu opens several sets of menus from which you can choose many various functions. The menus that open depend on what type of object you right-click, that is, a chassis object, a module, an interface, a PVC, or a profile.

Because there are so many variations of the Cisco DSL Manager object menus, illustrations of only some menu sets are included as examples in this section. A complete description of all the menus is provided in the "Summary of Cisco DSL Manager Object Menus" section on page C-6.

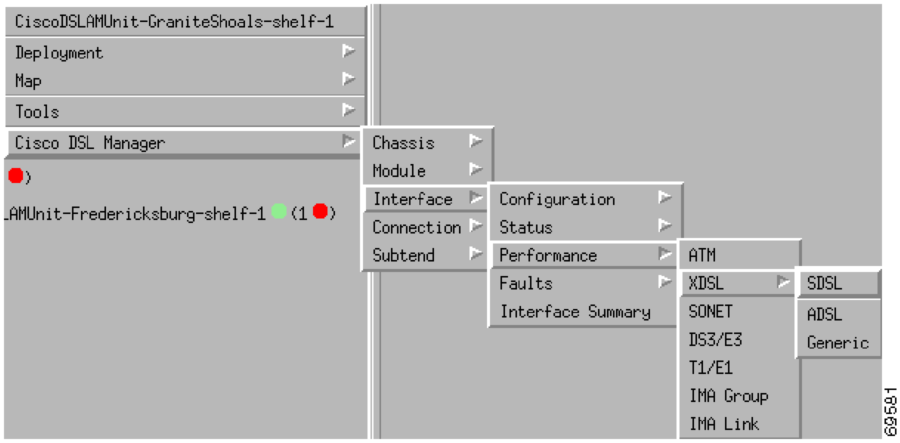
The Chassis Administration menu is shown in Figure C-1.

Figure C-1 Cisco DSL Manager Menu—Chassis Administration



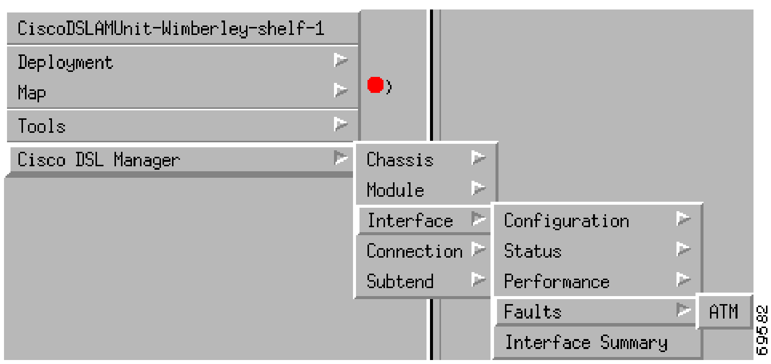
The Interface Performance menu that opens from a chassis is shown in Figure C-2.

Figure C-2 Cisco DSL Manager Menu—Interface Performance from a Chassis



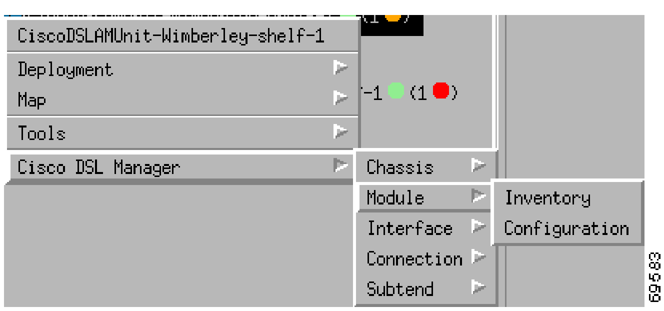
The Interface Faults menu is shown in Figure C-3.

Figure C-3 Cisco DSL Manager Menu—Interface Faults



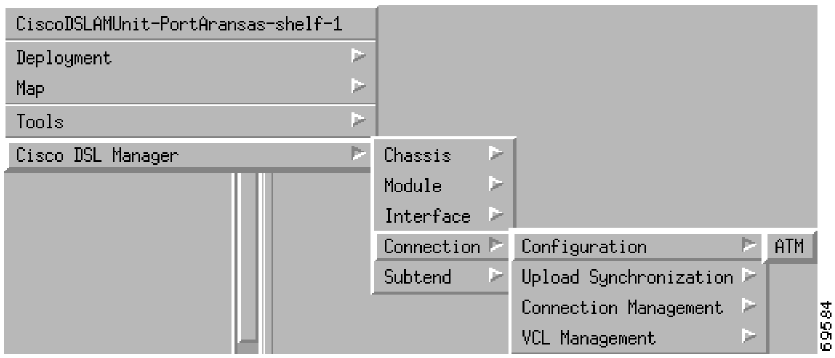
The Module Inventory and Module Configuration menu is shown in Figure C-4.

Figure C-4 Cisco DSL Manager Menu—Module Inventory and Configuration



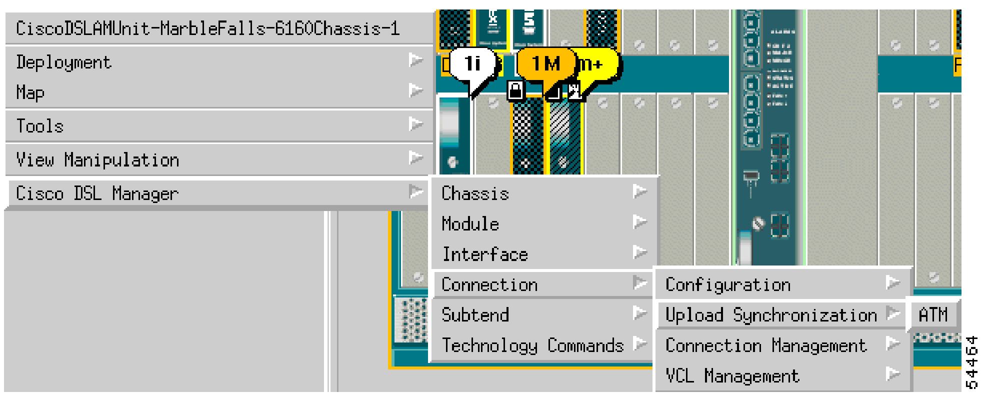
The Connection Configuration menu is shown in Figure C-5.

Figure C-5 Cisco DSL Manager Menu—Connection Configuration



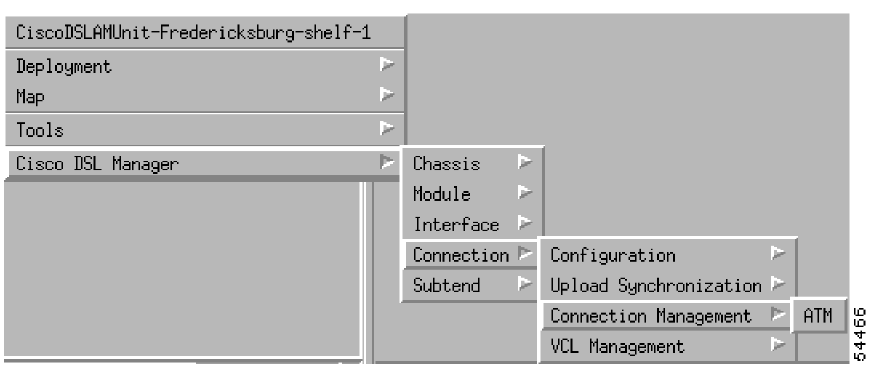
The Connection Upload Synch menu is shown in Figure C-6.

Figure C-6 Cisco DSL Manager Menu—Connection Upload Synch



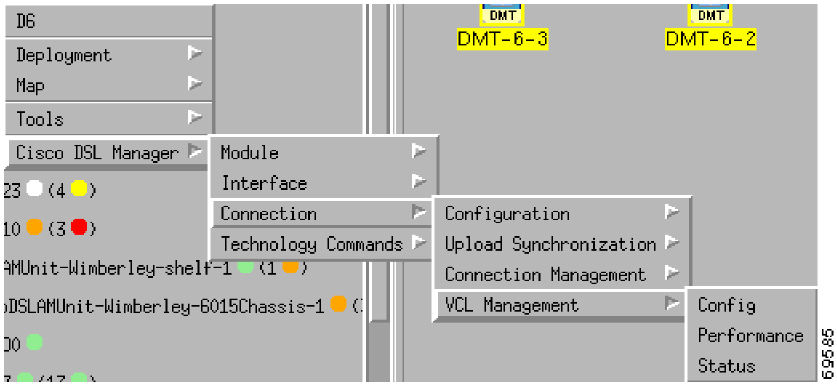
The Connection Management menu is shown in Figure C-7.

Figure C-7 Cisco DSL Manager Menu—Connection Management



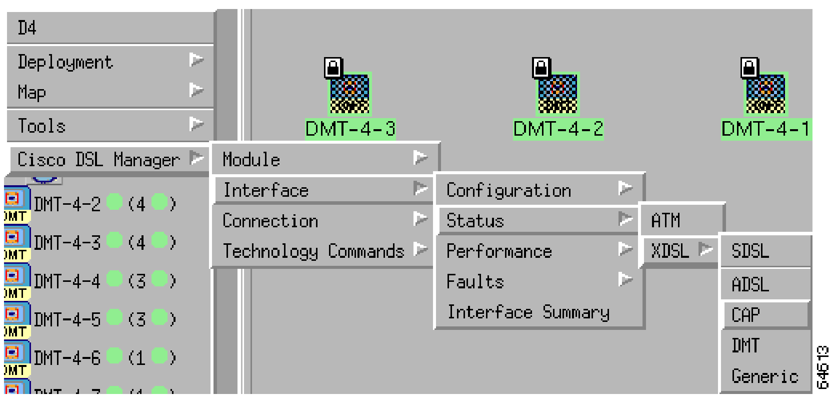
The VCL Management menu is shown in Figure C-8.

Figure C-8 Cisco DSL Manager Menu—VCL Management



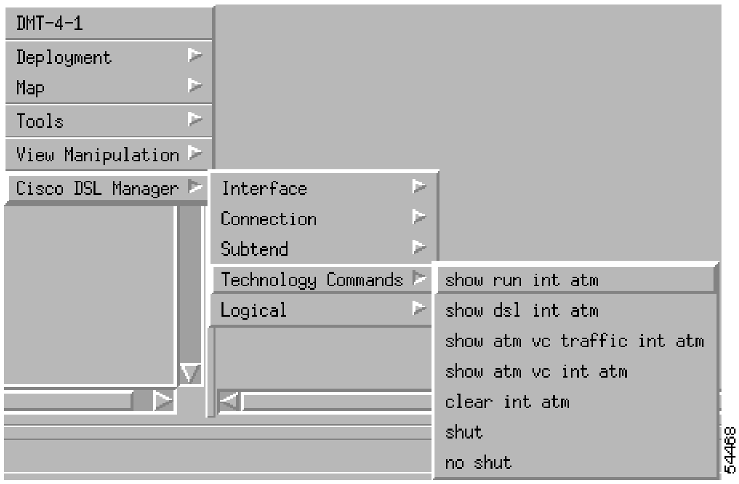
The Interface Status menu is shown in Figure C-9.

Figure C-9 Cisco DSL Manager Menu—Interface Status



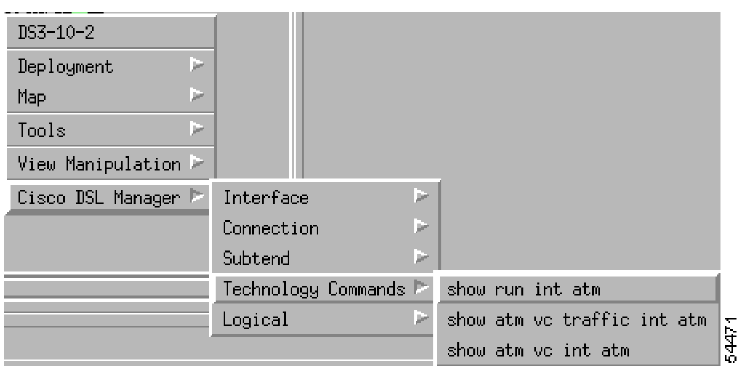
The Technology Commands menu, accessed through a DSLAM, is shown in Figure C-10. See the "Using the Technology Commands and Tools" section on page B-10 for more information about these commands.

Figure C-10 Cisco DSL Manager Menu—Technology Commands Through a DSLAM



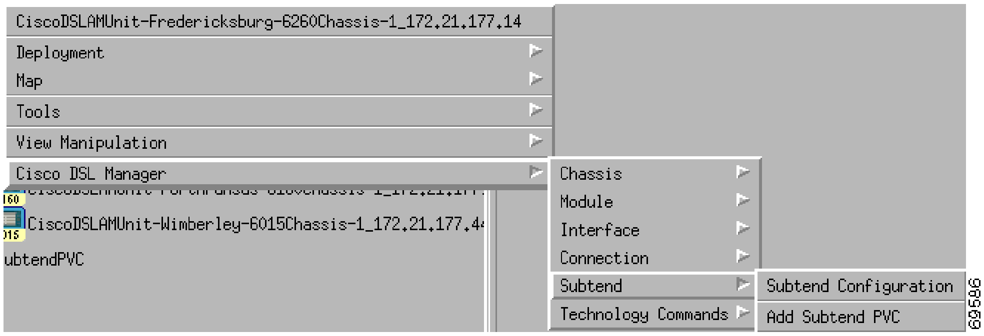
The Technology Commands menu, accessed through an interface, is shown in Figure C-11.

Figure C-11 Cisco DSL Manager Menu—Technology Commands Through an Interface



The Subtend menu is shown in Figure C-12.

Figure C-12 Cisco DSL Manager Menu—Subtend Menu



Note Remember, the menus that display from the Cisco DSL Manager object menu depend on the object from which you access the menus and the hierarchy view you are in when you right-click the object.

Summary of Cisco DSL Manager Object Menus

This section describes the sets of cascading menus that open when you right-click an object from the Map Viewer window and choose Cisco DSL Manager. It is from these menus that you access the CDM GUI windows in which you perform CDM functions and tasks. The sets of menus that open depend on whether you right-click a chassis (DSLAM) object, a module, an interface, a PVC or SPVC, or a profile.

This section includes the following topics:

- Chassis-Level Object Menus, page C-6
- Module-Level Object Menus, page C-10
- Interface-Level Object Menus, page C-12
- PVC or SPVC-Level Object Menus, page C-14
- Profile-Level Object Menus, page C-15

Chassis-Level Object Menus

When you access the Cisco DSL Manager menu from the chassis level, the following menus display:

- Chassis-Level Chassis Menus
- Chassis-Level Module Menus
- Chassis-Level Interface Menus
- Chassis-Level Connection Menus
- Chassis-Level Subtend Menus
- Chassis-Level Technology Commands Menus

Chassis-Level Chassis Menus

The menus that open from Chassis are described in Table C-1. The table lists the menu choices that display when you right-click a chassis (DSLAM) object. The left column lists the first level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from a chassis object you can choose **Cisco DSL Manager > Chassis > Administration > Management Information**, and the Management Information window opens.

Table C-1 Cisco DSL Manager Menu Descriptions—Chassis-Level Chassis Menus

Menu	Description
Administration	Management Information—Opens the Opens the Management Information window SNMP Settings—Opens the SNMP Management window IOS Image Download—Opens the IOS Image Download window Configuration Backup/Restore—Opens the Configuration Backup/Restore window Chassis Polling/Connection Policy—Opens the Chassis Polling/Connection Policy window
Configuration	Opens the Chassis Configuration window
Tools (Technology Specific Tools)	Telnet—Opens Telnet window Logging • View Error Log—Opens the Syslog Messages window • View Command History—Opens the Command Log window
Inventory	Opens the Chassis Inventory window
Fault Management	Opens the Chassis Fault Management window
Profile Management	xDSL Profiles—Opens XDSL Interface Manager window ATM Qos Profiles—Opens the ATM QoS Profiles Configuration window
Chassis Summary	Opens the Chassis Summary Data window

Chassis-Level Module Menus

The menus that open from Module are described in Table C-2. The table lists the menu choices that display when you right-click a chassis (DSLAM) object. The left column lists the first level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from a chassis object you can choose **Cisco DSL Manager > Module > Inventory**, and the Module Inventory window opens.

Table C-2 Cisco DSL Manager Menu Descriptions—Chassis-Level Module Menus

Menu	Description
Inventory	Opens the Module Inventory window
Configuration	Opens the Module Configuration window

Chassis-Level Interface Menus

The menus that open from Interface are described in Table C-3. The table lists the menu choices that display when you right-click a chassis (DSLAM) object. The left column lists the first-level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from a chassis object you can choose **Cisco DSL Manager > Interface > Configuration > ATM**, and the ATM Interface Configuration window opens.

Table C-3 Cisco DSL Manager Menu Descriptions—Chassis-Level Interface Menus

Menu	Description
Configuration	ATM—Opens the ATM Interface Configuration window *x*DSL—Opens the Apply XDSL Profile window DS3/E3—Opens the Manage DS3/E3 Interface Configuration window T1/E1—Opens the T1/E1 Interface Configuration window IMA Group—Opens the IMA Group Configuration window
Status	ATM—Opens the ATM Interface Status window XDSL: • SDSL—Opens the SDSL Interface Status window • ADSL—Opens the ADSL Interface Status window • CAP—Opens the CAP Interface Status window • DMT—Opens the DMT Interface Status window • Generic—Opens the Interface Status window SONET—Opens the SONET Interface Status window DS3/E3—Opens the DS3/E3 Interface Status window T1/E1—Opens the T1/E1 Interface Status window IMA Group—Opens the IMA Group Status window IMA Link—Opens the IMA Link Status window
Performance	ATM—Opens the ATM Interface Performance window XDSL: • SDSL—Opens the SDSL Interface Performance window • ADSL—Opens the ADSL Interface Performance window • Generic—Opens the Interface Performance window SONET—Opens the SONET Performance window DS3/E3—Opens the DS3/E3 Interface Performance window T1/E1—Opens the T1/E1 Performance window IMA Group—Opens the IMA Group Performance window IMA Link—Opens the IMA Link Performance window
Faults	ATM—Opens the ATM Interface Faults window
Interface Summary	Opens the Interface Summary window

Chassis-Level Connection Menus

The menus that open from Connection are described in Table C-4. The table lists the menu choices that display when you right-click a chassis (DSLAM) object. The left column lists the first-level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from a chassis object you can choose **Cisco DSL Manager > Connection > Configuration > ATM**, and the ATM QoS Profiles Management window opens.

Table C-4 Cisco DSL Manager Menu Descriptions—Chassis-Level Connection Menus

Menu	Description
Configuration	ATM—Opens the ATM QoS Profiles Management window
Upload Synchronization	ATM—Opens the ATM Connection Upload window
Connection Management	ATM—Opens the ATM Connection Management window
VCL Management	Config—Opens the ATM VCL Configuration window Performance—Opens the ATM VCL Configuration window Status—Opens the ATM VCL Configuration window

Chassis-Level Subtend Menus

The menus that open from Subtend are described in Table C-5. The table lists the menu choices that display when you right-click a chassis (DSLAM) object and the name of the window that opens when you choose that item. For example, from a chassis object you can choose **Cisco DSL Manager > Subtend > Subtend Configuration** and the Subtend Configuration window opens.

Table C-5 Cisco DSL Manager Menu Descriptions—Chassis-Level Subtend Menus

Menu	Description
Subtend Configuration	Opens the Subtend Configuration window
Add Subtend PVC	Opens the Add Subtend PVC window

Note To open the Delete Subtend PVC window, you must access the object menu from the subtend PVC that you want to delete and choose **Cisco DSL Manager > Subtend > Delete Subtend PVC**.

Chassis-Level Technology Commands Menus

The menus that open from Technology Commands are described in Table C-6. The table lists the menu choices that display when you right-click a chassis (DSLAM) object. The left column lists the first-level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from a chassis object you can choose **Cisco DSL Manager > Technology Commands > Save Running Config** and a Telnet session to the DSLAM opens.

Table C-6 Cisco DSL Manager Menu Descriptions—Chassis-Level Technology Commands Menus

Menu	Description
Save Running Config	Opens a Telnet session to the IP address of the DSLAM.
Check Alarms on the Chassis	Issues the show facility-alarm status command and transfer the IOS login user name and login password.
Set Chassis Temperature-rating as Commercial	Issues the set temperature rating command to for commercial Cisco 6015 DSLAMs. This is the default. A temperature rating mismatch alarm is triggered when any installed system component has a different temperature rating than the system temperature rating setting.
Set Chassis Temperature-rating as OSP	Issues the set temperature rating command for outside plant environment (OSP) Cisco 6015 DSLAMs.
Check Chassis Temperature-rating Status	Issues the show environment command and display information about system temperature settings.

Note You must set user name and password for a DSLAM before you use the technology commands that initiate a Telnet session to the IP address of the DSLAM.

Module-Level Object Menus

When you access the Cisco DSL Manager menu from the module level, the following menus display:

- Module-Level Module Menus
- Module-Level Interface Menus
- Module-Level Connection Menus
- Technology Commands Menu—reset card is the only choice

Module-Level Module Menus

The menus that open from Module are described in Table C-7. The table lists the menu choices that display when you right-click a module object and the name of the window that opens when you choose that item. For example, from a module object you can choose **Cisco DSL Manager > Module > Inventory** and the Module Inventory window opens.

Table C-7 Cisco DSL Manager Menu Descriptions—Module-Level Module Menus

Menu	Description
Inventory	Opens the Module Inventory window
Configuration	Opens the Configuration window

Module-Level Interface Menus

The menus that open from Interface are described in Table C-8. The table lists the menu choices that display when you right-click a module object and the name of the window that opens when you choose that item. For example, from a module object you can choose **Cisco DSL Manager >Interface > Configuration** and the ATM Interface window opens.

Table C-8 Cisco DSL Manager Menu Descriptions—Module-Level Interface Menus

Menu	Description
Configuration	ATM—Opens the ATM Interface Configuration window xDSL—Opens the Apply XDSL Profile window
Status	ATM—Opens the ATM Status window XDSL: • SDSL—Opens the SDSL Interface Status window • ADSL—Opens the ADSL Interface Status window • CAP—Opens the CAP Interface Status window • DMT—Opens the DMT Interface Status window • Generic—Opens the Interface Status window
Performance	ATM—Opens the ATM Interface Performance window XDSL: • SDSL—Opens the SDSL Performance window • ADSL—Opens the ADSL Interface Performance window • Generic—Opens the Interface Performance window
Faults	ATM—Opens the ATM Faults window
Interface Summary	Opens the Interface Summary window

Module-Level Connection Menus

The menus that open from Connection are described in Table C-9. The table lists the menu choices that display when you right-click a module object and the name of the window that opens when you choose that item. For example, from a module object you can choose **Cisco DSL Manager > Connection > Configuration > ATM** and the ATM QoS Profiles Management window opens.

Table C-9 Cisco DSL Manager Menu Descriptions—Module-Level Connection Menus

Menu	Description
Configuration	ATM—Opens the ATM QoS Profiles Management window
Upload Synch	ATM—Opens the ATM Upload Synch window
Connection Management	ATM—Opens the ATM Connection Management window
VCL Management	Config—Opens the ATM VCL Configuration window Performance—Opens the ATM VCL Configuration window Status—Opens the ATM VCL Configuration window

Interface-Level Object Menus

When you access the Cisco DSL Manager menu from the interface level, the following menus display:

- Interface-Level Object Menus
- Connection-Level Connection Menus
- Subtend Object Menu—Add Subtend PVC is the only choice
- Technology Commands Menu

Interface-Level Object Menus

The menus that open from Interface are described in Table C-10. The table lists the menu choices that display when you right-click an interface (line card or NI card) object. The left column lists the first-level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from an interface object you can choose **Cisco DSL Manager > Interface > Configuration > Configuration** and the ATM Interface Configuration window opens.

Table C-10 Cisco DSL Manager Menu Descriptions—Interface-Level Interface Menus

Menu	Description
Configuration	Configuration—Opens the ATM Interface Configuration window XDSL—Opens the Apply XDSL Profile window
Status	ATM—Opens the ATM Status window XDSL: • SDSL—Opens the SDSL Interface Status window • ADSL—Opens the ADSL Interface Status window • Status—Opens the CAP Interface Status window • DMT—Opens the DMT Interface Status window • Generic—Opens the Interface Status window
Performance	ATM—Opens the ATM Interface Performance window XDSL: ADSL—Opens the ADSL Interface Performance window
Faults	ATM—Opens the ATM Faults window
Interface Summary	Opens the Interface Summary window

Connection-Level Connection Menus

The menus that open from Connection are described in Table C-11. The table lists the menu choices that display when you right-click an interface (line card or NI card) object. The left column lists the first-level menus; the second column shows the second-level menu choices and the name of the window that opens when you choose that item. For example, from an interface object you can choose **Cisco DSL Manager > Connection > Configuration > ATM** and the ATM QoS Profiles Management window opens.

Table C-11 Cisco DSL Manager Menu Descriptions—Connection Level Connection Menus

Menu	Description
Configuration	ATM—Opens the ATM QoS Profiles Management window
Upload Synch	ATM—Opens the ATM Upload Synch window
Connection Management	ATM—Opens the ATM Connection Management window
VCL Management	Config—Opens the ATM VCL Configuration window Performance—Opens the ATM VCL Configuration window Status—Opens the ATM VCL Configuration window

Technology Commands Menu

The menu choices that display from Technology Commands menu issue IOS commands and open a Telnet session to the DSLAM IP address. You must have user name and password set to successfully initiate a Telnet session. Table C-12 describes the Interface Technology commands:

Table C-12 Technology Commands Menu

Menu Choice (Command)	Description
show run int[1] atm	Choose this item from an interface object (line card) to issue the show run int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.
show dsl int atm	Choose this item from an interface object (line card) to issue the show dsl int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.
show atm vc[2] traffic int atm	Choose this item from an interface object (line card), PVC, or SPVC object to issue the show atm vc traffic int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.
show atm vc int atm	Choose this item from an interface object (line card) to issue the show atm vc int atm command and transfer the IOS login user name, login password, enable password, slot number, and port number.
clear atm int	Choose this item from an interface object (line card) to issue the clear ATM int command and transfer the login user name, login password, slot number, and port number.
shut[3]	Choose this item from an interface object (line card) to issue the shut int atm command and transfer the login user name, login password, slot number, and port number.
no shut	Choose this item from an interface object (line card) to issue the no shut int atm command and transfer the login user name, login password, slot number, and port number.

1. int = interface
2. vc = virtual circuit (or connection)
3. shut = shutdown

PVC or SPVC-Level Object Menus

You access the Cisco DSL Manager menu from the PVC or SPVC level within the Component Managed view. The menus that display include:

- Connection
- Configuration > ATM—Opens the ATM Configuration window
- Upload Synch > ATM—Opens the ATM Upload Synch window
- Connection Management > ATM—Opens the ATM Connection Management window
- VCL Management

Profile-Level Object Menus

You access the Cisco DSL Manager menu from profiles within the Component Managed view. The set of menus that display include:

- Chassis > Profile Management > xDSL Profiles—Opens the XDSL Profile Management window
- Interface > Configuration > xDSL—Opens the XDSL Interface Configuration window

Finding Tasks and Related Windows

This appendix lists tasks for setting up and managing DSLAMs through the CDM GUI, identifies the associated windows, and includes links to the related procedures.

This appendix includes the following sections:

- CDM GUI Tasks and Related Procedures, page D-1
- GUI Windows and Related Procedures, page D-8

CDM GUI Tasks and Related Procedures

Table D-2 lists the windows, tabs, and related information and procedures that you do through these windows.

Table D-1 User Tasks

Topic/Procedure	Related Window
ATM QoS Profiles and PVC/SPVC Connections	
Opening the ATM QoS Profiles Configuration Window, page 4-8 Creating an ATM QoS Profile, page 4-10 Deleting an ATM QoS Profile, page 4-12 Applying an ATM QoS Profile to a PVC or SPVC, page 4-36	ATM QoS Profiles Configuration
Activating the PVC or SPVC Connection, page 4-37	ATM Connections Management
Managing VCLs, page 4-39	ATM VCL Configuration
Manually Uploading ATM QoS Profiles, page 4-49	ATM Connection Upload
Back up and Restore	
Backing Up and Restoring Configuration Information, page 6-8	Configuration Backup/Restore
Commissioning and Configuration	
Commissioning a Cisco DSLAM Chassis, page 2-31	Chassis Configuration

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
Commissioning Cards, page 2-35	Configuration
Setting Chassis Information in the Management Information Window, page 2-28 Setting the Cisco IOS Command Line Security Password, page 2-30	Information Management
Commissioning a Cisco DSLAM Chassis, page 2-31	Chassis Configuration
Commissioning Cards, page 2-35	Configuration
Creating ATM QoS Profiles, page 4-8	ATM QoS Profiles Configuration
Configuring ATM Interfaces, page 2-36	ATM Interface Configuration
Configuring an E3 Interface, page 2-45	DS3/E3 Interface Configuration
Configuring the T1/E1 Interface, page 2-43	T1/E1 Interface Configuration
Configuring a VCL, page 4-39	ATM VCL Configuration
Configuring IMA Groups, page 4-52	IMA Group Configuration
Connecting the Children DSLAMs, page 5-8 Discovering the System Topology of a Subtend Configuration, page 5-11 Setting Up a Subtend Configuration Using an NI-2 DSLAM as Parent and NI-1 DSLAMs as Children, page 5-13 Disconnecting Two DSLAMs from a Subtend Configuration, page 5-14	Subtend
Backing Up and Restoring Configuration Information, page 6-8	Configuration Backup and Restore
Deleting Objects	
Deleting Network Elements, page 2-49	Deployment Wizard
Deleting Subtend PVCs, page 5-19	Delete Subtend PVC

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
Deployment	
Deployment Process, page 2-7 Deploying a Generic Site, page 2-8 Manually Deploying a Cisco DSLAM Chassis, page 2-13 Manually Deploying a Line Card, page 2-19 Creating PVCs and SPVCs, page 4-12 Creating ATM PVCs, page 4-13 Deploying ATM SPVCs with a Cisco EMF Endpoint, page 4-21 Deploying an ATM SPVC with a non-Cisco EMF Endpoint, page 4-27 Deploying ATM SPVCs with a Cisco EMF Endpoint, page 4-21	Deployment Wizard
***x*DSL Profiles**	
Viewing xDSL Profiles, page 3-22 Applying xDSL Profiles, page 3-24	Apply XDSL Profile
Using the Sync Profile Feature, page 3-5 Creating a New Profile from an Existing Profile, page 3-6 Setting New DMT Parameters, page 3-8 DMT Tab Field Definitions, page 3-10 Setting the Interleaved Channel Fields, page 3-13 Setting the Fast Channel Parameters, page 3-14 Setting the Rate Adaptation Parameters, page 3-14 Setting the Downstream/Upstream Parameters, page 3-15 Setting the Common Parameters, page 3-15 Setting New SDSL/G.SHDSL Parameters, page 3-15 SDSL/G.SHDSL Tab Field Descriptions, page 3-17 Setting New CAP Parameters, page 3-18 CAP Tab Field Definitions, page 3-20	XDSL Interface Manager
Downloading IOS and Setting IOS Passwords	
Downloading a Cisco IOS Software Image, page 6-10	IOS Download Image
Specifying Chassis Information and Setting the Cisco IOS Passwords, page 2-28 Setting the DSLAM IOS Password, page 5-5 Setting Telnet Passwords, page 6-7	Management Information

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
Historical Performance	
Viewing Historical Performance Data, page 8-50 Setting the Chassis to Performance Logging On State, page 8-50 Viewing DS3/E3 or OC-3 Interface Performance Data, page 8-51 Viewing ATM over ADSL over DMT Interface Performance Data, page 8-56 Performance Window Line Chart Tab, page 8-53 Performance Window Bar Chart Tab, page 8-54 Performance Window Table Display Tab, page 8-55	Performance (historical)
IMA	
Using Inverse Multiplexing over ATM on Cisco 6015, 6160, and 6260 DSLAMs, page 4-51 Overview of IMA, page 4-51 Configuring IMA Groups, page 4-52	IMA Group Configuration
Inventory	
Viewing the Chassis Inventory Window—General Tab, page 9-3 Viewing the Chassis Inventory Window—Asset Tracking Tab, page 9-4	Chassis Inventory
Viewing the Module Inventory Window—General Tab, page 9-6 Viewing the Module Inventory Window—Asset Tracking Tab, page 9-8	Module Inventory
Log Files	
Viewing and Configuring the Command Log Window, page 6-4 Command Log Window Field Descriptions, page 6-6	Command Log
Configuring the System Log Message Details, page 6-2 SysLog Messages Window Field Descriptions and Severity Level Descriptions, page 6-3	Syslog Messages
Performance Data	
Viewing the ADSL Interface Performance Window—Line Performance (1) Tab, page 8-10 Viewing the ADSL Interface Performance Window—Line Performance (2) Tab, page 8-12 Viewing the ADSL Interface Performance Window—Fast Channel Performance (1) Tab, page 8-14 Viewing the ADSL Interface Performance Window—Fast Channel Performance (2) Tab, page 8-16 Viewing the ADSL Interface Performance Window—Interleave Channel Performance (1) Tab, page 8-18 Viewing the ADSL Interface Performance Window—Interleave Channel Performance (2) Tab, page 8-20	ADSL Interface Performance

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
Viewing ATM Interface Performance Data, page 8-34 Viewing the ATM Interface Performance Window Transmitted and Received Areas, page 8-36 Viewing the ATM Interface Performance Connection Established Area, page 8-39	ATM Interface Performance
Viewing T1/E1 Interface Performance Data, page 8-28	T1/E1 Interface Performance
Viewing ATM Interface Faults, page A-4	ATM Interface Faults
Viewing ATM VCL Performance, page 4-45	ATM VCL Performance
Viewing DS3/E3 Interface Performance Data, page 8-30	DS3/E3 Interface Performance
Viewing IMA Group Performance Data, page 8-39	IMA Group Performance
Viewing IMA Link Performance Data, page 8-41	IMA Link Performance
Viewing Current Performance Data in the Interface Performance Windows, page 8-1 Viewing xDSL Interface Performance Data, page 8-3	Interface Performance
Viewing CPU Performance Data of NI Cards, page 8-2	Module Performance
Viewing the SDSL Performance Window Current 15 Minutes Tab, page 8-23 Viewing the SDSL Performance Window Current 1 Day Tab, page 8-24 Viewing the SDSL Performance Window Previous 1 Day Tab, page 8-25 Viewing the SDSL Performance Window Agent Reset Tab, page 8-27	SDSL Performance
Viewing the SONET Interface Performance Window—Section Tab, page 8-46 Viewing the SONET Interface Performance Window—Line Tab, page 8-47 Viewing the SONET Interface Performance Window—Path Tab, page 8-49	SONET Interface Performance
Polling	
Setting Polling Intervals, page 4-3	Chassis Polling/Connection Policy
SNMP Traps	
Enabling SNMP Trap Generation, page 2-47	SNMP Management
Status	
Viewing ADSL Interface Status, page 7-19	ADSL Interface Status

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
Viewing ATM Interface Status, page 7-10	ATM Interface Status
Viewing Chassis Fault Management Status, page 7-1	Chassis Fault Management
Viewing DMT Interface Status, page 7-23 Viewing the DMT Interface Status Window—Line Tab, page 7-24 Viewing the DMT Interface Status Window—Channel Tab, page 7-27	DMT Interface Status
Viewing DS3/E3 Interface Status, page 7-7	DS3/E3 Interface Status
Viewing FlexiCAP Interface Status, page 7-36	CAP Interface Status
Viewing Generic Interface Status, page 7-3	Interface Status
Viewing IMA Group and Link Status on Cisco 6015, 6160, and 6260 DSLAMs, page 7-14 Viewing the IMA Group Status Window, page 7-14	IMA Group Status
Viewing IMA Group and Link Status on Cisco 6015, 6160, and 6260 DSLAMs, page 7-14 Viewing the IMA Link Status Window, page 7-17	IMA Link Status
Viewing SDSL and G.SHDSL Interface Status, page 7-34	SDSL Interface Status
Viewing the SONET Interface Status Window—Medium Tab, page 7-30 Viewing the SONET Interface Status Window—Section Tab, page 7-31 Viewing the SONET Interface Status Window—Line Tab, page 7-32 Viewing the SONET Interface Status Window—Path Tab, page 7-33	SONET Interface Status
Viewing T1/E1 Interface Status, page 7-5	T1/E1 Interface Status
Viewing VCL Status, page 4-47	ATM VCL Status
Subtending	
Setting Up Subtended Subscribers, page 5-16 Setting Subscriber PVCs on a Subtend System, page 5-16	Add Subtend PVC

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
Overview of Subtend Configurations, page 5-1 Guidelines for Configuring a Subtend System, page 5-3 Setting the DSLAM IOS Password, page 5-5 Preparing IOS Configurations, page 5-6 Creating a Child DSLAM Using Telnet, page 5-7 Connecting the Children DSLAMs, page 5-8 Deploying a Parent DSLAM, page 5-10 Using CDM to Configure a Subtend System, page 5-11 Discovering the System Topology of a Subtend Configuration, page 5-11 Setting Up a Subtend Configuration Using an NI-2 DSLAM as Parent and NI-1 DSLAMs as Children, page 5-13 Disconnecting Two DSLAMs from a Subtend Configuration, page 5-14 Setting Up Subtended Subscribers, page 5-16	Subtend Configuration
Summary Data	
Using the Filter Operation, page 9-10 Using the Find Operation, page 9-10 Using the Sort Operation, page 9-11 Viewing Data in the Chassis Summary Data Window—View Ports Tab, page 9-11 Viewing Data in the Chassis Summary Data Window—View Subscriber PVCs Tab, page 9-12 Viewing Data in the Chassis Summary Data Window—View Equipment Tab, page 9-14	Chassis Summary
Viewing the Interface Summary Window—Summary Tab, page 9-16 Viewing the Interface Summary Window—Connections Tab, page 9-17 Viewing the Interface Summary Window—SNMP Errors Tab, page 9-18	Interface Summary
Synchronization	
Synchronizing Alarms and Saving the Running Configuration, page 4-4 Overview of the Connection Synchronization Policy, page 4-5 Setting the Connection Synchronization Policy, page 4-6 Saving the Running Configuration to Memory, page 6-12 Synchronizing Alarms, page 6-13	Chassis Polling/ Connection Policy

Table D-1 User Tasks (continued)

Topic/Procedure	Related Window
VCLs	
Managing VCLs, page 4-39 Configuring a VCL, page 4-39 Using the ATM VCL Configuration Window—Configuration Tab, page 4-39 Description of the ATM VCL Configuration Window—Configuration Tab, page 4-42	ATM VCL Configuration

GUI Windows and Related Procedures

Table D-2 lists the windows, tabs, and related information and procedures that you do through these windows.

Table D-2 Windows and Their Related Procedures

Add Subtend PVC window
Setting Up Subtended Subscribers, page 5-16 Setting Subscriber PVCs on a Subtend System, page 5-16
ADSL Interface Performance window
Viewing the ADSL Interface Performance Window—Line Performance (1) Tab, page 8-10 Viewing the ADSL Interface Performance Window—Line Performance (2) Tab, page 8-12 Viewing the ADSL Interface Performance Window—Fast Channel Performance (1) Tab, page 8-14 Viewing the ADSL Interface Performance Window—Fast Channel Performance (2) Tab, page 8-16 Viewing the ADSL Interface Performance Window—Interleave Channel Performance (1) Tab, page 8-18 Viewing the ADSL Interface Performance Window—Interleave Channel Performance (2) Tab, page 8-20
ADSL Interface Status window
Viewing the ADSL Interface Status Window—Line Tab, page 7-21 Viewing the ADSL Interface Status Window—Channel Tab, page 7-22
Apply XDSL Profile window
Viewing xDSL Profiles, page 3-22 Applying xDSL Profiles, page 3-24
ATM Connections Management window
Activating the PVC or SPVC Connection, page 4-37
ATM Connection Upload window
Manually Uploading ATM QoS Profiles, page 4-49
ATM Interface Configuration window
Configuring ATM Interfaces, page 2-36

Table D-2 Windows and Their Related Procedures (continued)

ATM Interface Faults window
Viewing ATM Interface Faults, page A-4
ATM Interface Performance window
Viewing ATM Interface Performance Data, page 8-34 Viewing the ATM Interface Performance Window Transmitted and Received Areas, page 8-36 Viewing the ATM Interface Performance Connection Established Area, page 8-39
ATM Interface Status window
Viewing ATM Interface Status, page 7-10
ATM QoS Profiles Configuration window
Creating ATM QoS Profiles, page 4-8 Opening the ATM QoS Profiles Configuration Window, page 4-8 Creating an ATM QoS Profile, page 4-10 Deleting an ATM QoS Profile, page 4-12 Applying an ATM QoS Profile to a PVC or SPVC, page 4-36 Opening the ATM QoS Profiles Configuration Window, page 4-8
ATM VCL Configuration window
Managing VCLs, page 4-39 Configuring a VCL, page 4-39 Using the ATM VCL Configuration Window—Configuration Tab, page 4-39 Description of the ATM VCL Configuration Window—Configuration Tab, page 4-42
ATM VCL Performance window
Viewing ATM VCL Performance, page 4-45
ATM VCL Status window
Viewing VCL Status, page 4-47
CAP Interface Status window
Viewing FlexiCAP Interface Status, page 7-36
Chassis Configuration window
Commissioning a Cisco DSLAM Chassis, page 2-31 Synchronizing Alarms and Saving the Running Configuration, page 4-4 Overview of the Connection Synchronization Policy, page 4-5 Saving the Running Configuration to Memory, page 6-12 Synchronizing Alarms, page 6-13
Chassis Fault Management window
Viewing Chassis Fault Management Status, page 7-1
Chassis Inventory window
Viewing the Chassis Inventory Window—General Tab, page 9-3 Viewing the Chassis Inventory Window—Asset Tracking Tab, page 9-4

Table D-2 Windows and Their Related Procedures (continued)

Chassis Polling/Connection Policy window
Setting Polling Intervals, page 4-3 Setting the Connection Synchronization Policy, page 4-6
Chassis Summary window
Using the Filter Operation, page 9-10 Using the Find Operation, page 9-10 Using the Sort Operation, page 9-11 Viewing Data in the Chassis Summary Data Window—View Ports Tab, page 9-11 Viewing Data in the Chassis Summary Data Window—View Subscriber PVCs Tab, page 9-12 Viewing Data in the Chassis Summary Data Window—View Equipment Tab, page 9-14
Command Log window
Viewing and Configuring the Command Log Window, page 6-4 Command Log Window Field Descriptions, page 6-6
Configuration window
Commissioning Cards, page 2-35
Configuration Backup/Restore window
Backing Up and Restoring Configuration Information, page 6-8
Delete Subtend PVC window
Deleting Subtend PVCs, page 5-19
DMT Interface Status window
Viewing DMT Interface Status, page 7-23 Viewing the DMT Interface Status Window—Line Tab, page 7-24 Viewing the DMT Interface Status Window—Channel Tab, page 7-27
DS3/E3 Interface Configuration window
Configuring an E3 Interface, page 2-45
DS3/E3 Interface Performance window
Viewing DS3/E3 Interface Performance Data, page 8-30
DS3/E3 Interface Status window
Viewing DS3/E3 Interface Status, page 7-7
IMA Group Configuration window
Using Inverse Multiplexing over ATM on Cisco 6015, 6160, and 6260 DSLAMs, page 4-51 Overview of IMA, page 4-51 Configuring IMA Groups, page 4-52
IMA Group Performance window
Viewing IMA Group Performance Data, page 8-39
IMA Group Status window
Viewing IMA Group and Link Status on Cisco 6015, 6160, and 6260 DSLAMs, page 7-14 Viewing the IMA Group Status Window, page 7-14

Table D-2 Windows and Their Related Procedures (continued)

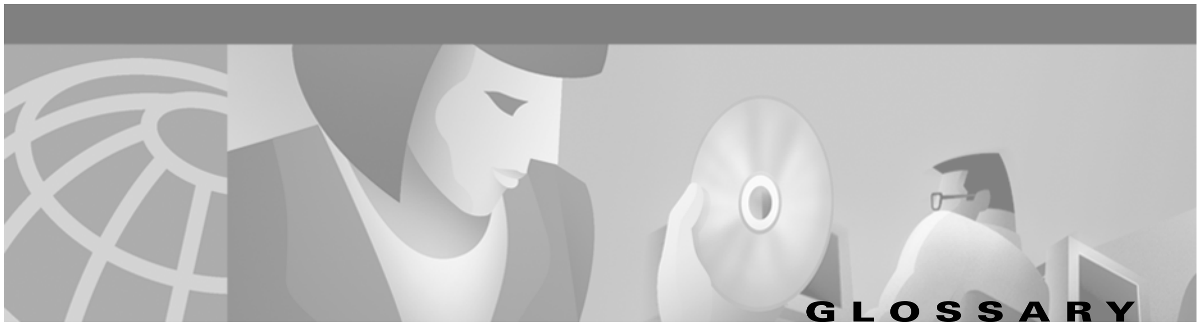
IMA Link Performance window
Viewing IMA Link Performance Data, page 8-41
IMA Link Status window
Viewing IMA Group and Link Status on Cisco 6015, 6160, and 6260 DSLAMs, page 7-14 Viewing the IMA Link Status Window, page 7-17
Interface Performance window
Viewing Current Performance Data in the Interface Performance Windows, page 8-1 Viewing xDSL Interface Performance Data, page 8-3
Interface Status window
Viewing Generic Interface Status, page 7-3
Interface Summary window
Viewing the Interface Summary Window—Summary Tab, page 9-16 Viewing the Interface Summary Window—Connections Tab, page 9-17 Viewing the Interface Summary Window—SNMP Errors Tab, page 9-18
IOS Download Image window
Downloading a Cisco IOS Software Image, page 6-10
Management Information window
Specifying Chassis Information and Setting the Cisco IOS Passwords, page 2-28 Setting the DSLAM IOS Password, page 5-5 Setting Telnet Passwords, page 6-7
Module Inventory window
Viewing the Module Inventory Window—General Tab, page 9-6 Viewing the Module Inventory Window—Asset Tracking Tab, page 9-8
Module Performance window
Viewing CPU Performance Data of NI Cards, page 8-2
Performance (historical) window
Viewing Historical Performance Data, page 8-50 Setting the Chassis to Performance Logging On State, page 8-50 Viewing DS3/E3 or OC-3 Interface Performance Data, page 8-51 Viewing ATM over ADSL over DMT Interface Performance Data, page 8-56 Performance Window Line Chart Tab, page 8-53 Performance Window Bar Chart Tab, page 8-54 Performance Window Table Display Tab, page 8-55
SDSL Interface Status window
Viewing SDSL and G.SHDSL Interface Status, page 7-34

Table D-2 Windows and Their Related Procedures (continued)

SDSL Performance window
Viewing the SDSL Performance Window Current 15 Minutes Tab, page 8-23
Viewing the SDSL Performance Window Current 1 Day Tab, page 8-24
Viewing the SDSL Performance Window Previous 1 Day Tab, page 8-25
Viewing the SDSL Performance Window Agent Reset Tab, page 8-27
SNMP Management window
Enabling SNMP Trap Generation, page 2-47
SONET Interface Performance window
Viewing the SONET Interface Performance Window—Section Tab, page 8-46
Viewing the SONET Interface Performance Window—Line Tab, page 8-47
Viewing the SONET Interface Performance Window—Path Tab, page 8-49
SONET Interface Status window
Viewing the SONET Interface Status Window—Medium Tab, page 7-30
Viewing the SONET Interface Status Window—Section Tab, page 7-31
Viewing the SONET Interface Status Window—Line Tab, page 7-32
Viewing the SONET Interface Status Window—Path Tab, page 7-33
Subtend Configuration window
Overview of Subtend Configurations, page 5-1
Guidelines for Configuring a Subtend System, page 5-3
Setting the DSLAM IOS Password, page 5-5
Preparing IOS Configurations, page 5-6
Creating a Child DSLAM Using Telnet, page 5-7
Connecting the Children DSLAMs, page 5-8
Deploying a Parent DSLAM, page 5-10
Using CDM to Configure a Subtend System, page 5-11
Discovering the System Topology of a Subtend Configuration, page 5-11
Setting Up a Subtend Configuration Using an NI-2 DSLAM as Parent and NI-1 DSLAMs as Children, page 5-13
Disconnecting Two DSLAMs from a Subtend Configuration, page 5-14
Setting Up Subtended Subscribers, page 5-16
Syslog Messages window
Configuring the System Log Message Details, page 6-2
SysLog Messages Window Field Descriptions and Severity Level Descriptions, page 6-3
T1/E1 Interface Configuration window
Configuring the T1/E1 Interface, page 2-43
T1/E1 Interface Performance window
Viewing T1/E1 Interface Performance Data, page 8-28

Table D-2 Windows and Their Related Procedures (continued)

T1/E1 Interface Status window
Viewing T1/E1 Interface Status, page 7-5
XDSL Interface Manager window
Using the Sync Profile Feature, page 3-5 Creating a New Profile from an Existing Profile, page 3-6 Setting New DMT Parameters, page 3-8 DMT Tab Field Definitions, page 3-10 Setting the Interleaved Channel Fields, page 3-13 Setting the Fast Channel Parameters, page 3-14 Setting the Rate Adaptation Parameters, page 3-14 Setting the Downstream/Upstream Parameters, page 3-15 Setting the Common Parameters, page 3-15 Setting New SDSL/G.SHDSL Parameters, page 3-15 SDSL/G.SHDSL Tab Field Descriptions, page 3-17 Setting New CAP Parameters, page 3-18 CAP Tab Field Definitions, page 3-20



GLOSSARY

Numerics

2B1Q 2 binary 1 quaternary. An encoding scheme that provides a 2 bits per baud, 80k baud per second, 160kbps transfer rate. The most common signaling method on ISDN U interfaces.

4B3T 4 binary 3 ternary. A baseband line code (modulation and signaling structure) that maps a group of four binary bits into true three-state ternary code, achieving a baud-rate reduction of 25 percent. This line code technique is used to support ISDN Basic Rate Interface (BRI) in European countries. The corresponding line code used in the US to support ISDN BRI is 2B1Q.

4xDMT quad-port DMT ATU-C line card. Supports four ADSL modem connections and DMT line encoding. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

4xDMT over ISDN quad-port DMT ATU-C over ISDN line card. Supports four ADSL modem connections. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

4xflexi quad-port flexi ATU-C line card. Supports four ADSL modem connections and CAP, DMT, and G.lite line encoding. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

4xSDSL quad-port STU-C line card. Supports four SDSL modem connections and 2B1Q line encoding. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

8xDMT octal-port DMT ATU-C line card. Supports eight ADSL modem connections and DMT line encoding. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

8xDMT over ISDN octal-port DMT ATU-C over IDSN line card. Supports eight ADSL modem connections and DMT over ISDN protocols that employ 2B1Q- or 4B3T-based encoding.

8xG.SHDSL octal-port SHTU-C line card. Supports eight G.SHDSL modem connections and TC-PAM line encoding. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

8xIDSL octal-port ITU-C line card. Supports eight IDSL modem connections, or four connections when the chassis limits the number of tip and ring connectors. Supports 2B1Q line encoding. For chassis compatibility, refer to the *Cisco DSLAM Compatibility Notes* or the appropriate hardware installation guide.

A

AAL ATM adaptation layer. AAL is an adaptation layer within the data link layer of the OSI model. AAL is divided into a segmentation and reassembly sublayer (SAR) and a convergence sublayer. The SAR divides the application datastream into transmit cells and then reassembles the received cells into a datastream that is compatible with the related application. The convergence sublayer specifies the requirements for the various types of applications that run over ATM. AAL is defined in terms of types, 1 to 5, specified by the type of traffic that it supports. Each type offers an appropriate QoS.

ABR available bit rate. A QoS class defined by the ATM Forum for ATM networks. ABR is used for connections that do not require timing relationships between source and destination. ABR provides no guarantees in terms of cell loss or delay, providing only best-effort service. Traffic sources adjust their transmission rate in response to information they receive describing the status of the network and its capability to successfully deliver data. Compare with *CBR*, *UBR*, and *VBR*.

accounting management One of five categories of network management defined by ISO for the management of ISO networks. Accounting management subsystems are responsible for collecting network data that relates to resource usage. See also *configuration management*, *fault management*, *performance management*, and *security management*.

address Data structure or logical convention used to identify a unique entity, such as a particular process or network device.

ADSL asymmetric digital subscriber line. An *x*DSL technology in which more bandwidth is delivered downstream (from the CO to the customer site) than upstream over a single copper twisted pair. Compare with *IDSL*, *SDSL*, and *SHDSL*. See also *DSL*.

alarm A notification that a traffic signal has degraded or failed or that equipment is malfunctioning. See also *event* and *trap*.

AM amplitude modulation. A modulation technique by which information is conveyed through the amplitude of the carrier signal. Compare with *FM* and *PAM*. See also *modulation*.

American National Standards Institute See *ANSI*.

American Wire Gauge See *AWG*.

amplitude modulation See *AM*.

ANSI American National Standards Institute. An organization that coordinates, develops, and approves international and U.S. standards for, among other things, communications and networking. ANSI is a member of ISO. See also *ISO*.

APS automatic protection switching. A method that allows transmission equipment to recover automatically from failures, such as a cut cable.

asymmetric digital subscriber line See *ADSL*.

asynchronous communications A method of transmitting data in which individual characters are encapsulated in control bits (called start and stop bits) that designate the beginning and end of each character. Asynchronous transmission allows communication without precise clocking.

Asynchronous Transfer Mode See *ATM*.

ATM Asynchronous Transfer Mode. The international standard for cell relay in which multiple service types (voice, video, or data, for example) are transmitted in fixed-length (53-byte) cells. ATM offers fast packet technology, and real-time, demand-led switching for efficient use of network resources.

ATM adaptation layer See *AAL*.

ATU-C See *xTU-C*.

ATU-R See *xTU-R*.

authentication In security, the verification of the identity of a person or a process.

autodiscovery The process by which a network device automatically searches through a range of network addresses and discovers the known types of devices that are present. Also see *subrack discovery.*

automatic protection switching See *APS*.

available bit rate See *ABR*.

AWG American Wire Gauge. The standard gauge for measurement of thickness of a wire in the United States.

B

backplane The physical connection between an interface processor or card and the data buses and the power distribution buses inside a DSLAM.

bandwidth The difference between the highest and lowest frequencies available for network signals. The term also is used to describe the rated throughput capacity of a given network medium or protocol. For a digital channel, this is defined in bits. For an analog channel, it depends on the type and method of modulation used to encode the data.

bandwidth on demand The ability of a user to dynamically set upstream and downstream line speeds to a particular rate of speed.

BITS building integrated timing supply. A clock in a CO that supplies DS1 or composite clock timing references to all synchronous network elements in that office.

bits per second See *bps*.

bootflash Separate Flash memory device used primarily to store the Cisco IOS boot image, operational Cisco IOS images, and system configuration information.

BOOTP Bootstrap Protocol. The protocol used by a network node to determine the IP address of its Ethernet interfaces to affect network booting.

Bootstrap Protocol See *BOOTP*.

bps bits per second. A standard measurement of digital transmission speeds.

bridge A device that connects two or more physical networks and forwards packets between them. Bridges can usually be made to filter packets, that is, to forward only certain traffic. See *switch* and *router*.

broadband In telecommunications, any channel having a bandwidth greater than a voice-grade channel (4 kHz).

broadband remote access server Device that terminates remote users at the corporate network or Internet users at the internet service provider (ISP) network that provides firewall, authentication, and routing services for remote users.

broadcast Data packet that are sent to all nodes on a network. Broadcasts are identified by a broadcast address. Compare with *multicast* and *unicast*.

building integrated timing supply See *BITS*.

bus topology A linear method of connecting devices so that transmissions from network stations propagate the length of the medium and are received by all other stations. Compare with *daisy-chain topology*, *ring topology*, *star topology*, and *tree topology*.

C

CAP Carrierless Amplitude and Phase Modulation. A bandwidth efficient transmission technology for implementing DSL. The transmit and receive signals are modulated into two wide-frequency bands using passband modulation techniques. CAP supports ADSL and RADSL line coding.

Carrierless Amplitude and Phase Modulation See *CAP*.

CBOS Cisco Broadband Operating System. The operating system that users access to configure and operate the Cisco 600 Series DSL CPE products.

CBR constant bit rate. A QoS class defined by the ATM Forum for ATM networks. CBR is used for connections that depend on precise clocking to ensure undistorted delivery. Compare with *ABR*, *UBR*, and *VBR*.

CDM Cisco DSL Manager. An SNMP-based element management system with fault, configuration, and performance reporting capabilities. CDM runs within the Cisco EMF and manages DSLAMs through a GUI.

central office See *CO*.

chassis The cage or housing into which cards or modules are installed. See also *DSLAM* and *multiplexer*.

child See *subtended node chassis*.

Cisco Broadband Operating System	See *CBOS*.
Cisco DSL Manager	See *CDM*.
Cisco Element Management Framework	See *Cisco EMF*.
Cisco EMF	Cisco Element Management Framework. The element management layer of the system. Cisco EMF provides the framework to support carrier-class element managers across Cisco service provider product lines.
Cisco IOS	Cisco system software that provides common functionality, scalability, and security for all products under the CiscoFusion architecture. Cisco IOS is a CLI that allows centralized, integrated, and automated installation and management of internetworks while ensuring support for a wide variety of protocols, media, services, and platforms.
Cisco Service Management	See *CSM*.
CLEI	common language equipment identifier. The standard code used by suppliers to identify equipment parts and system configurations. CLEI is a registered trademark of Bellcore (now Telcordia).
CLI	command line interface. An interface that allows the user to interact with the operating system by entering commands and optional arguments.
client	Node or software program (front-end device) that requests services from a server.
CLLI	common language location identifier.
CO	central office. A local telephone company office at all local loops in a given area connect and where the circuit switching of subscriber lines occurs.
command line interface	See *CLI*.
common language equipment identifier	See *CLEI*.
common language location identifier	See *CLLI*.
community string	Text string that acts as a password used with SNMP protocol. The password is used to authenticate messages and can be read-only or have read/write privileges; setting it to read-only is private and setting it to read-write is public. A community string is case sensitive.
configuration management	One of five categories of network management defined by ISO for the management of OSI networks. Configuration management subsystems are responsible for detecting and determining the state of a network. See also *accounting management*, *fault management*, *performance management*, and *security management*.

configuration register In Cisco DSLAMs, a 16-bit, user-configurable value that determines how the DSLAM functions during initialization. The configuration register can be stored in hardware or software. In hardware, the bit position is set using a jumper. In software, the bit position is set by specifying a hexadecimal value using configuration commands.

connectionless network A type of communications network in which no logical connection (for example, no leased line or dialed-up channel) is required between sending and receiving stations. Compare with *connection-oriented network*.

connection-oriented network A type of communications network in which data transfer requires the establishment of a virtual circuit. Compare with *connectionless network*.

constant bit rate See *CBR*.

CPE customer premises equipment. Terminating equipment, such as terminals, telephones, and modems, supplied by the telephone company. The equipment is installed at customer sites and connected to the telephone company network.

CSM Cisco Service Management system of OAM&P and management tools for service providers and large enterprise networks.

customer premises equipment See *CPE*.

D

daemon A program that is not invoked explicitly but lies dormant waiting for some condition(s) to occur.

daisy-chain topology A method of connecting devices in a series so that signals are passed through the chain from one device to the next. Unlike a ring topology, the last device in the series is not connected to the first. Compare with *bus topology*, *ring topology*, *star topology*, and *tree topology*.

data circuit-terminating equipment See *DCE*.

data storage backup Process of making a copy of the data that resides on a server.

data terminal equipment See *DTE*.

DCE Data circuit-terminating equipment (ITU-T expansion). Devices and connections of a communications network that comprise the network end of the user-to-network interface. The DCE provides a physical connection to the network, forwards traffic, and provides a clocking signal used to synchronize data transmissions between DCE and DTE devices. Modems and interface cards are examples of DCE. Compare with *DTE*.

DDTS Distributed Defect Tracking System. Cisco tracks bugs in a variety of products, including router software, communication server software, and network management software, using a system called DDTS. DDTS is also used for bugs in some hardware and microcode products, and for bugs in some internal tools, including the automated test software and various Software Tools.

destination address Address of a network device that is receiving data. See also *source address*.

DHCP Dynamic Host Configuration Protocol. Provides a mechanism to allocate IP addresses dynamically so that addresses can be reused when hosts no longer need them. Defined in RFC 2131.

digital signal level 3 See *DS3*.

digital subscriber line See *DSL*.

digital subscriber line access multiplexer See *DSLAM*.

Discrete Multitone See *DMT*.

Distributed Defect Tracking System See *DDTS*.

distributed server Server that supports a specific group of users on the network. Also referred to as local or workgroup server.

DMT Discrete Multitone. A technology that uses digital signal processors for transmission. DMT supports ADSL line coding.

downstream Data that is coming from the NI-2 card to the subscriber lines. See also *upstream*.

DS3 digital signal level 3. A framing specification used for transmitting digital signals at 44.736 Mbps on a T3 facility. See also *E3*.

DSL digital subscriber line. Public network technology that delivers high bandwidth over conventional copper wiring at limited distances. There are several types of DSL: ADSL, IDSL, SDSL, and SHDSL, to name a few. All are provisioned via modem pairs, with one modem located at a CO and the other at the customer site. Because most DSL technologies do not use the whole bandwidth of the twisted pair, there is room remaining for a voice channel. See also *ADSL*, *IDSL*, *SDSL*, and *SHDSL*.

DSL Forum An organization of competing companies that sponsors an Internet Web site (http://www.adsl.com) containing information about the applications, technology, systems, market, trials, and tariffs related to DSL technology.

DSLAM digital subscriber line access multiplexer. A device that connects many digital subscriber lines to a network by multiplexing the DSL traffic onto one or more network trunk lines. The Cisco DSLAMs include the Cisco 6015, Cisco 6100, Cisco 6130, Cisco 6160, and Cisco 6260. See also *chassis* and *multiplexer*.

DTE data terminal equipment. Device at the user end of a user-network interface that serves as a data source, destination, or both. DTE connects to a data network through a DCE device (for example, a modem) and typically uses clocking signals generated by the DCE. DTE includes such devices as computers, protocol translators, and multiplexers. Compare with *DCE*.

Dynamic Host Configuration Protocol See *DHCP*.

E

E1 Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 2.048 Mbps. See also *T1*.

E3 Wide-area digital transmission scheme used predominantly in Europe that carries data at a rate of 34.368 Mbps. See also *DS3* and *T3*.

EFCI explicit forward congestion indication. In ATM, one of the congestion feedback modes allowed by ABR service. EFCI is set by a network element to notify the destination end-system of congestion or impending congestion in the network.

EIA Electronic Industries Alliance. A standards organization made up of electronics industry organizations. EIA is responsible for the RS-232C and RS-422 standards.

Electronic Industries Alliance See *EIA*.

electrostatic discharge See *ESD*.

encapsulation The wrapping of data in a particular protocol header. For example, Ethernet data is wrapped in a specific Ethernet header before network transit. Also, when bridging a dissimilar network, the entire frame from one network is placed in the header used by the data link layer protocol of the other network.

EPROM Erasable programmable read-only memory. Nonvolatile memory chips that are programmed after they are manufactured, and, if necessary, can be erased by some means and reprogrammed.

erasable programmable read-only memory See *EPROM*.

error detection A process used during file transfer to discover discrepancies between transmitted and received data. Some file transfer programs only detect errors; others detect errors and attempt to fix them (called error correction).

ESD electrostatic discharge. Discharge of stored static electricity that can damage electronic equipment and impair electrical circuitry, resulting in complete or intermittent failures.

ESF Extended Superframe. A framing type that is used on T1 circuits that consists of 24 frames of 192 bits each, with the 193rd bit providing timing and other functions.

Ethernet One of the most common LAN wiring schemes, Ethernet has a transmission rate of 10 Mbps; a newer standard called Fast Ethernet has a rate of 100 Mbps.

ETSI European Telecommunications Standards Institute. ETSI is a non-profit organization producing voluntary telecommunications standards used throughout Europe, some of which have been adopted by the european community as the technical base for Directives or Regulations.

European Telecommunications Standards Institute See *ETSI*.

event Network message indicating operational irregularities in physical elements of a network or a response to the occurrence of a significant task, typically the completion of a request for information. See also *alarm* and *trap*.

explicit forward congestion indication See *EFCI*.

Extended Superframe See *ESF*.

F

fault management One of five categories of network management defined by ISO for management of OSI networks. Fault management attempts to ensure that network faults are detected and controlled. See also *accounting management*, *configuration management*, *performance management*, and *security management*.

FCC Federal Communications Commission. A U.S. government agency that regulates interstate and foreign communications. The FCC sets rates for communication services, determines standards for equipment, and controls broadcast licensing.

Federal Communications Commission See *FCC*.

ferrite Use on coaxial cables to reduce the radiation/EMI susceptibility to high frequency noise.

field replaceable unit See *FRU*.

File Transfer Protocol See *FTP*.

firmware Software instructions set permanently or semi-permanently in ROM.

flash memory A special type of EPROM that can be used and reprogrammed in blocks instead of one byte at a time.

FM frequency modulation. Modulation technique in which signals of different frequencies represent different data values. Compare with *AM* and *PAM*. See also *modulation*.

frame A packet as it is transmitted over a serial line. The term derives from character-oriented protocols that involved the addition of special start-of-frame and end-of-frame characters for packet transmission.

frequency modulation See *FM*.

FRU field replaceable unit. Hardware component that can be removed and replaced on-site. Typical FRUs include cards, modules, PEMs, and some chassis components. When FRUs are removed from the chassis, service is interrupted for some or all of the system.

FTP File Transfer Protocol. The application protocol used to transfer files between network nodes.

G

G.dmt Pseudonym for G.992.1.

G.lite Pseudonym for G.992.2.

G.SHDSL See *SHDSL*.

graphical user interface See *GUI*.

GUI graphical user interface. A user environment that uses pictorial as well as textual representations of the input and the output of applications and the hierarchical or other data structure in which information is stored.

H

handshake See *hs*.

HDLC High-Level Data Link Control. Bit-oriented synchronous data link layer protocol developed by ISO. Derived from Synchronous Data Link Control (SDLC), HDLC specifies a data encapsulation method on synchronous serial links using frame characters and checksums.

header (1) The protocol control information that is located at the beginning of a protocol data unit. (2) The portion of a message that contains information to guide the message to the correct destination and contains, for example, sender and receiver addresses and routing instructions.

High-Level Data Link Control See *HDLC*.

host Computer system on a network. Similar to the term node, except that host usually implies a computer system; node generally applies to any networked system, including access servers and routers. See also *node*.

hot swapping Feature that permits the addition, replacement, or removal of cards or modules without interrupting the system power, entering console commands, or causing other software or interfaces to shut down. Sometimes called “online insertion and removal” or “power-on servicing.” Removal of some cards causes interruption to some or all of the system.

hs handshake. Sequence of messages that are exchanged between two or more network devices to ensure transmission synchronization.

I

I/O card or I/O module input/output card or module.

ICP cell IMA control protocol cell. IMA control protocol cell used for aligning the cells in multiple links.

IDSL	ISDN digital subscriber line. An *x*DSL technology that uses ISDN technology to deliver data. Compare with *ADSL*, *SDSL*, and *SHDSL.* See also *DSL*.
IEEE	Institute of Electrical and Electronics Engineers. A U.S. publishing and standards organization responsible for many LAN standards.
IMA	inverse multiplexing over ATM. A standard protocol defined by the ATM Forum in 1997.
IMA control protocol cell	See *ICP cell*.
IMA group	Physical links grouped to form a higher-bandwidth logical link the rate of which is approximately the sum of the individual link rates.
industrial temperature	See *ITEMP.*
Institute of Electrical and Electronics Engineers	See *IEEE*.
Integrated Services Digital Network	See *ISDN*.
intermixing	Installation of line cards with different modulation types into a single DSLAM. Intermixing rules are determined by spectral frequency overlap considerations, chassis type, and line card modulation type.
International Organization for Standardization	See *ISO*.
International Telecommunication Union Telecommunication Standardization Sector	See *ITU-T.*
inverse multiplexing	Process whereby physical links are grouped to form a higher-bandwidth logical link whose rate is approximately the sum of the individual link rates.
inverse mutliplexing over ATM	See *IMA*.
ISDN	Integrated Services Digital Network. Communication protocol offered by telephone companies that permits telephone networks to carry data, voice, and other source traffic.
ISDN digital subscriber line	See *IDSL*.
ISO	International Organization for Standardization. A voluntary, nontreaty organization founded in 1946 that is responsible for creating international standards in many areas, including computers and communications.
ITEMP	industrial temperature.

ITU-C See *xTU-C*.

ITU-R See *xTU-R*.

ITU-T International Telecommunication Union Telecommunication Standardization Sector. ITU-T is the telecommunication standardization sector of ITU and is responsible for making technical recommendations about telephone and data (including fax) communications systems for service providers and suppliers.

J

jitter In telecommunications, analog communication line distortion caused by the variation of a signal from its reference timing positions. Jitter can cause data loss, particularly at high speeds.

L

LAN local-area network. High-speed, low-error data network covering a relatively small geographic area (up to a few thousand meters). LANs connect workstations, peripherals, terminals, and other devices in a single building or other geographically limited area. LAN standards specify cabling and signaling at the physical and data link layers of the OSI model. Ethernet, FDDI, and Token Ring are widely used LAN technologies. Compare with *WAN*.

laser light amplification by stimulated emission of radiation. Analog transmission device in which a suitable active material is excited by an external stimulus to produce a narrow beam of coherent light that can be modulated into pulses to carry data. Networks based on laser technology are sometimes run over SONET.

LED light emitting diode. The lights indicate status or activity of electronic equipment.

light emitting diode See *LED*.

line rate The speed at which data is transferred over a particular line type, expressed in bps.

link Network communications channel that consists of a circuit or transmission path and all related equipment between a sender and a receiver. In a transmission network, a link is a point-to-point connection between adjacent nodes.

local-area network See *LAN*.

logical port A logical entry to a server machine. Logical ports are mostly invisible to the user, though you may occasionally see a URL with a port number included in it. These ports do not refer to physical locations; they are set up by server administrators for network trafficking.

loopback A diagnostic test that returns the transmitted signal to the sending device after the signal has passed through a network or across a particular link. The returned signal can then be compared to the transmitted one and the discrepancies between the two can be used to trace the fault. When you are trying to locate a faulty piece of equipment, you can repeat loopbacks, eliminating satisfactory machines, until the problem is found.

M

managed object In network management, a network device that can be managed by a network management protocol.

Management Information Base See *MIB*.

maximum rate Maximum total data throughput allowed on a given virtual circuit. The maximum rate, which cannot exceed the media rate, represents the highest data throughput the virtual circuit will ever deliver, measured in bps or cells per second.

MIB Management Information Base. A collection of objects that can be accessed through a network management protocol, such as SNMP or Common Management Information Protocol (CMIP).

MMF multimode fiber. Optical fiber that supports the propagation of multiple frequencies of light. See also *SMF.*

modulation Process by which the characteristics of electric signals are transformed to represent information. Types of modulation include AM, FM, and PAM. See also *AM*, *FM*, and *PAM*.

multicast Single packets copied by the network and sent to a specific subset of network addresses. Compare with *broadcast* and *unicast*.

multimode fiber See *MMF*.

multiplexer Equipment that enables several data streams to be sent over a single physical line. A device for combining several channels to be carried by one line or fiber. See also *chassis* and *DSLAM*.

N

NAT Network Address Translation. Mechanism for reducing the need for globally unique IP addresses. NAT allows an organization with addresses that are not globally unique to connect to the Internet by translating those addresses into globally routable address space.

NEBS Network Equipment Building Systems. An extensive set of performance, quality, environmental and safety requirements developed by Bellcore (now Telcordia).

network Collection of computers, printers, routers, switches, and other devices that can communicate with each other over some transmission medium.

Network Address Translation See *NAT*.

network element A network element is generally a combination hardware and software system that is designed primarily to perform a telecommunications service function.

Network Equipment Building Systems See *NEBS*.

network management Generic term used to describe systems or actions that help maintain, characterize, or troubleshoot a network.

network management system See *NMS*.

network timing reference See *NTR*.

NI-2 card A second generation network interface card for Cisco DSLAMs. Board that works with the network software and operating systems to transmit and receive messages on a network.

NMS network management system. A system responsible for managing at least part of a network. An NMS communicates with agents to help keep track of network statistics and resources.

node Endpoint of a network connection or a junction common to two or more lines in a network. Nodes can be processors, controllers, or workstations. Nodes can be interconnected by links and serve as control points in the network. Node sometimes is used generically to refer to any entity that can access a network, and frequently is used interchangeably with device. See also *host*.

node system save file See *NSS file*.

noise margin Noise margin is the margin between the signal and noise in decibels (dB). The recommended minimum noise margin is typically 6dB. The 6dB noise margin was specified based on empirical research and the resulting algorithms to allow the best performance (line rate and reach) while maintaining the 10-7 bit-error rate. When RADSL is enabled for a DSL DMT application, the modem will train to 1) the specified rate or 2) the highest rate possible given the line conditions while maintaining a 6dB margin.

nonvolatile random-access memory See *NVRAM*.

NSS file node system save file. The file that is saved during the Save Configuration procedure or during a software download. This file is required for the Restore Configurations procedure.

NVRAM nonvolatile random-access memory. RAM that retains its contents when a unit is powered off.

O

OAM&P operations, administration, management, and provisioning. Provides the facilities and the personnel required to manage a network.

OC Optical Carrier. Series of physical protocols (OC-1, OC-2, OC-3, and so on) defined for SONET optical signal transmissions. OC signal levels put STS frames onto multimode fiber-optic line at a variety of speeds. The base rate is 51.84 Mbps (OC-1); each signal level thereafter operates at a speed divisible by that number (thus, OC-3 runs at 155.52 Mbps). See also *SONET* and *STS-3c*.

OC-*n* SONET optical carrier, Level *n* (such as *n* equals 3, 12, 48, 192).

Open System Interconnection See *OSI*.

operations, administration, management, and provisioning See *OAM&P*.

Operations Support System See *OSS*.

octal-port DMT ATU-C line card See *8xDMT*.

octal-port DMT ATU-C over IDSN line card See *8xDMT over ISDN*.

octal-port ITU-C line card See *8xIDSL*.

octal-port SHTU-C line card See *8xG.SHDSL*.

Optical Carrier See *OC*.

optical fiber See *MMF* and *SMF*.

OSI Open System Interconnection. An international standardization program created by ISO and ITU-T to develop standards for data networking that facilitate multivendor equipment interoperability. See also *ISO*.

OSS Operations Support System. Network management system supporting a specific management function, such as alarm surveillance and provisioning, in a carrier network.

P

PAM pulse amplitude modulation. Modulation scheme where a continuous analog signal is represented with a series of discrete analog samples, which are then recreated as a complete signal. Sampling allows several signals to be combined on a channel that would otherwise carry only one signal. Compare with *AM* and *FM*. See also *modulation*.

parent See *subtending host chassis*.

PEM power entry module. A hardware module that distributes power throughout a DSLAM.

performance management One of five categories of network management defined by ISO for the management of ISO networks. Performance management subsystems are responsible for analyzing and controlling network performance, including network throughput and error rates. See also *accounting management*, *configuration management*, *fault management*, and *security management*.

permanent virtual circuit See *PVC*.

permanent virtual connection See *PVC*.

permanent virtual path See *PVP*.

physical port A physical connection to a computer through which data flows. An Ethernet port, for example, is the point at which the Ethernet network cabling plugs into a computer.

plain old telephone service See *POTS*.

Point-to-Point Protocol See *PPP*.

port An interface on an internetworking device (such as a DSLAM).

POTS plain old telephone service. General term referring to the variety of telephone networks and services in place worldwide.

POTS splitter A device that enables both a DSL data device and a standard analog device to share the same ADSL or IDSL line.

power entry module See *PEM*.

PPP Point-to-Point Protocol. The successor to SLIP that provides router-to-router and host-to-network connections over both synchronous and asynchronous circuits. See *SLIP*.

protocol A formal description of messages to be exchanged and rules to be followed so that two or more systems can exchange information.

pulse amplitude modulation See *PAM*.

PVC permanent virtual circuit (or connection). A virtual circuit that is permanently established. PVCs save bandwidth associated with circuit establishment and tear down in situations where certain virtual circuits must exist all the time. Compare with SVC. See also *virtual circuit*.

PVP permanent virtual path. A virtual path that consists of PVCs. See also *PVC* and *virtual path*.

Q

QoS quality of service. A measure of performance for a transmission system that reflects its transmission quality and service availability.

quad-port DMT ATU-C over IDSN line card See *4xDMT over ISDN*.

quad-port flexi ATU-C line card See *4xflexi*.

quad-port STU-C line card See *4xSDSL*.

quality of service See *QoS*.

R

RADIUS Remote Authentication Dial-In User Service. A client/server security protocol created by Livingston Enterprises. Security information is stored in a central location, known as the RADIUS server.

RADSL rate adaptive digital subscriber line. A transmission technology that supports adaptive transmission rates through the use of intelligent DSL modems, which negotiate the line rate according to line conditions and profile specifications. Once the line rate is negotiated, the rate is locked when the line trains. RADSL supports both asymmetric and symmetric applications on a single twisted pair telephone line. See *ADSL*.

RAM random-access memory. Volatile memory that can be read and written by a microprocessor.

random-access memory See *RAM*.

Rate Adaptive Digital Subscriber Line See *RADSL*.

read-only memory See *ROM*.

redundancy In internetworking, the duplication of devices, services, or connections so that, in the event of failure, the redundant devices, services, or connections can perform the work of those that failed.

remote address The IP address of a remote server.

Remote Authentication Dial-In User Service See *RADIUS*.

remote monitoring See *RMON*.

remote server A network computer that allows a user to log on to the network from a distant location.

Request for Comments See *RFC*.

RFC Request for Comments. The document series, begun in 1969, which describes the Internet suite of protocols and related experiments. Not all RFCs describe Internet standards, but all Internet standards are written up as RFCs.

ring topology A method of connecting devices so that a series of repeaters is connected to one another by unidirectional transmission links to form a single closed loop. Each station on the network connects to the network at a repeater. Compare with *bus topology*, *daisy-chain topology*, *star topology*, and *tree topology*.

RMON remote monitoring. MIB agent specification described in RFC 1271 that defines functions for the remote monitoring of networked devices. The RMON specification provides numerous monitoring, problem detection, and reporting capabilities.

ROM read-only memory. Nonvolatile memory that can be read, but not written, by the microprocessor.

router A system responsible for making decisions about which of several paths network (or Internet) traffic will follow. The router uses a routing protocol to gain information about the network and algorithms to choose the best route based on several criteria known as "routing metrics." See also *bridge* and *switch.*

routing table A table that is stored in a router or some other internetworking device that keeps tracks of routes to particular network destinations, and, in some cases, metrics associated with those routes. A routing table is used to select the most appropriate route to forward information.

S

scalability Capacity of a network to keep pace with changes and growth.

SDSL symmetrical digital subscriber line. An *x*DSL technology that can deliver 1.168 Mbps downstream and upstream over a single copper twisted pair. Compare with *ADSL*, *IDSL*, and *SHDSL*. See also *DSL*.

security management One of five categories of network management defined by ISO for the management of ISO networks. Security management subsystems are responsible for controlling access to network resources. See also *accounting management*, *configuration management*, *fault management*, and *performance management*.

Serial Line Internet Protocol See *SLIP*.

server Node or software program that provides services to clients.

SHDSL single-pair high-speed digital subscriber line, also known as symmetric high bit rate digital subscriber loop. Compare with *ADSL*, *IDSL*, and *SDSL.* See also *DSL*.

shielded twisted pair A pair of insulated wires which are twisted together in a spiral manner. In addition, the pair is wrapped with metallic foil or braid, designed to insulate the pair from electromagnetic interference. Sometimes referred to as STP. See also *twisted pair* and *unshielded twisted pair.*

SHTU-C See *xTU-C*.

SHTU-R See *xTU-R*.

signal-to-noise ratio See *SNR*.

Simple Network Management Protocol See *SNMP*.

single-mode fiber See *SMF*.

single-pair high-speed digital subscriber line See *SHDSL*.

SLIP Serial Line Internet Protocol. A standard protocols for point-to-point serial connections using a variation of TCP/IP. This protocol is the predecessor of PPP. See *PPP* and *TCP*.

slot A numbered location within a chassis, which is capable of housing a card or module.

SMF single-mode fiber. Fiber-optic cabling with a narrow core that allows light to enter only at a single angle. Such cabling has higher bandwidth than multimode fiber, but requires a light source with a narrow spectral width (for example, a laser). See also *MMF*.

SNMP Simple Network Management Protocol. The network management protocol of choice for TCP/IP-based internets. SNMP provides a means to monitor and control network devices, and to manage configurations, statistics collection, performance, and security.

SNR signal-to-noise ratio. The usable signal being transmitted divided by the noise or undesired signal. SNR is a measure of transmission quality.

SONET Synchronous Optical Network. A standard format for transporting a wide range of digital communications services over optical fiber. SONET is characterized by standard line rates, optical interfaces, and signal formats.

source address Address of a network device that sends data. See also *destination address*.

star topology A method of connecting devices in which end points on a network are connected to a common central switch by point-to-point links. Compare with *bus topology*, *daisy-chain topology*, *ring topology*, and *tree topology*.

STM-1 Synchronous Transfer Module 1. Synchronous Digital Hierarchy standard for transmission over OC-3c optical fiber at 155.52 Mbps.

STS-3c Synchronous Transport Signal level 3, concatenated. SONET format that specifies the frame structure for the 155.52 Mbps-lines used to carry ATM cells. See also *SONET*.

STU-C See *xTU-C*.

STU-R See *xTU-R*.

subinterface One of a number of virtual interfaces on a single physical interface.

subnet For routing purposes, IP networks can be divided into logical subnets by means of a subnet mask. Values below those of the mask are valid addresses on the subnet.

subnet address Portion of an IP address that is specified as the subnetwork by the subnet mask.

subnet mask The 32-bit address mask used in IP to indicate the bits of an IP address that are being used for the subnet address.

subrack discovery The process by which a DSLAM node automatically searches through the interfaces and ports within that DSLAM and discovers the components that are present within that DSLAM.

subscriber A logical entity with attributes identifying the customer that is receiving service on a particular port.

subtended configuration Services and aggregates the data from one or more chassis into a subtending host chassis requiring only one connection to the outside network. This reduces the number of ATM edge-switch ports necessary to terminate multiple chassis.

subtended node chassis Downstream chassis in a subtended network configuration. Also known as the *child*.

subtending See *subtended configuration*.

subtending host chassis Provides the data network interface for the subtended node chassis and connects to the ATM backbone. Also known as the *parent*.

SVC switched virtual circuit (or connection). A virtual circuit that is dynamically established on demand and is torn down when transmission is complete. SVCs are used in situations where data transmission is sporadic. Compare with *PVC*. See also *virtual circuit*.

switch Network device that filters, forwards, and floods frames based on the destination address of each frame. The switch operates at the data link layer of the OSI model. See also *bridge* and *router*.

switched virtual circuit See *SVC*.

symmetric high bit rate digital subscriber loop See *SHDSL*.

symmetrical digital subscriber line See *SDSL*.

synchronous communications Data is not sent in individual bytes, but as frames of large data blocks.

Synchronous Optical Network See *SONET*.

Synchronous Transfer Module 1 See *STM-1*.

Synchronous Transport Signal level 3, concatenated See *STS-3c*.

SYSLOG SYSLOG allows you to log significant system information to a remote server.

T

T1 A digital carrier that is used to transmit a DS1 formatted digital signal at 1.544 Mbps through the telephone-switching network. See also *E1*.

T1.413 The ANSI standard for line coding and framing for full rate ADSL.

T3 A digital carrier that is used to transmit a DS3 formatted digital signal at 45 Mbps through the telephone-switching network. Compare with *E3*. See also *DS3*.

TC-PAM trellis coded pulse amplitude modulation. Trellis coding provides forward error correction, while pulse amplitude modulation is a modulation scheme where a continuous analog signal is represented with a series of discrete analog samples.

TCP Transmission Control Protocol. The major transport protocol in the Internet suite of protocols providing reliable, connection-oriented, full-duplex streams. See *SLIP*.

Telnet The virtual terminal protocol in the Internet suite of protocols. It allows users of one host to log in to a remote host and use resources as if they were connected to a local system.

TFTP Trivial File Transfer Protocol. A simple file transfer protocol (a simplified version of FTP) that allows files to be transferred from one computer to another over a network. TFTP does not offer password security.

tip and ring A pair of wires that provide the electrical connection between a telephone set and the local CO. The more electrically positive side of a POTS telephone line (0 V) is the tip. Its counterpart is the ring, which is the more negative side, 52 v).

topology Physical arrangement of network nodes and media within a networking structure.

trailer A block of information that is transmitted at the end of a message to trace error impacts and missing blocks.

training The handshake procedure that initiates and establishes an end-to-end *x*DSL connection

training mode The mode, either standard or quick, that a DSLAM port employs when it is training to a CPE. The training mode uses RADSL technology to adjust line speed according to noise conditions on the transmission line.

Transmission Control Protocol See *TCP*.

trap Message sent by SNMP agent to an NMS, a console, or a terminal to indicate the occurrence of a significant event, such as a specifically defined condition or a threshold that was reached. See also *alarm* and *event*.

tree topology A method of connecting devices that is similar to a bus topology, except that tree networks can contain branches with multiple nodes. Transmissions from a station propagate the length of the medium and are received by all other stations. Compare with *bus topology*, *daisy-chain topology*, *ring topology*, and *star topology*.

trellis coded pulse amplitude modulation See *TC-PAM*.

trellis encoding A channel coding technique which provides forward error correction capability.

Trivial File Transfer Protocol See *TFTP*.

twisted pair Two insulated copper wires twisted together with the twists or lays varied in length to reduce potential signal interference between the pairs.

U

UBR unspecified bit rate. A QoS class defined by the ATM Forum for ATM networks. UBR allows any amount of data up to a specified maximum to be sent across the network but there are no guarantees in terms of cell loss rate and delay. Compare with *ABR*, *CBR*, and *VBR*.

UDP User Datagram Protocol. A connectionless transport protocol that runs on top of the TCP/IP. UDP, like TCP, uses IP for delivery; however, unlike TCP, UDP provides for exchange of datagrams without acknowledgments or guaranteed delivery. This protocol is the best suited for small, independent requests, such as requesting a MIB value from an SNMP agent, in which setting up a connection would take more time than sending the data.

UL Underwriters Laboratories. A private organization that tests and certifies electrical components and devices against rigorous safety standards. A UL Listing Mark on a product means that representative samples of the product have been tested and evaluated against nationally recognized safety standards with regard to fire, electric shock, and other related safety hazards, and have met the standards.

Underwriters Laboratories See *UL*.

UNI User-Network Interface.

UNI signaling User-Network Interface signaling for ATM communications.

unicast Message sent to a single network destination. Compare with *broadcast* and *multicast*.

unshielded twisted pair Four-pair wire medium used in a variety of networks. Sometimes referred to as UTP. See also *shielded twisted pair* and *twisted pair*.

unspecified bit rate See *UBR*.

upstream Data that is coming from the subscriber lines to the NI-2 card. See also downstream.

User-Network Interface See *UNI*.

User Datagram Protocol See *UDP*.

V

variable bit rate See *VBR*.

VBR variable bit rate. A QoS defined by the ATM Forum for ATM networks. VBR is subdivided into a real time (rt) class and non-real time (nrt) class. VBR-rt is used for connections in which there is a fixed timing relationship between samples. VBR-nrt is used for connections in which there is no fixed timing relationship between samples but that still need a guaranteed QoS. Compare with *ABR*, *CBR*, and *UBR*.

VCC virtual channel connection. A logical circuit, made up of links, that carries data between two endpoints in an ATM network. It is sometimes called a virtual circuit connection. See also *VCI* and *VPI*.

VCI virtual channel identifier. A 16-bit field in the header of an ATM cell. The VCI, together with the VPI, is used to identify the next destination of a cell as it passes through to the ATM switch. It is sometimes called virtual circuit identifier. See also *VPI*.

virtual channel connection See *VCC*.

virtual channel identifier See *VCI*.

virtual circuit A logical circuit created to ensure reliable communication between two network devices. A virtual circuit is defined by a VPI/VCI pair and can be either PVC or SVC. In ATM, a virtual circuit is called a virtual channel. See also PVC, SVC, VCI, and VPI.

virtual circuit connection See *VCC*.

virtual circuit identifier See *VCI*.

virtual connection In ATM, a connection between end users that has a defined route and endpoints. See also *PVC* and *SVC*.

virtual path A logical grouping of virtual circuits that connect two sites. One of two types of ATM circuits identified by a VPI. A virtual path is a bundle of virtual circuits, all of which are switched across a network based on a common VPI. See also *VPI*.

virtual path identifier See *VPI*.

VPI virtual path identifier. An 8-bit field in the header of an ATM cell. The VPI, together with the VCI, is used to identify the next destination of a cell as it passes through the network. See also *VCI*.

W

WAN wide-area network. A data communications network that serves users across a broad geographic area and often uses transmission devices provided by common carriers. Compare with *LAN*.

WAN Interface Card See *WIC*.

WIC WAN Interface Card. A WIC card plugs into the card slot of a router and allows DSL use on routers. Each WIC acts as a CPE and can handle the amount of data available depending on the line conditions and the DSL profile assigned to the port.

wide-area network See *WAN*.

X

***x*DSL** Generic term used to refer to digital subscriber line equipment and services, including ADSL, IDSL, SDSL, and SHDSL. All are digital technologies that provide high bandwidth over existing copper infrastructure provided by the telephone companies.

***x*DSL Transmission Unit—central office** See xTU-C.

***x*DSL Transmission Unit—remote** See xTU-R.

***x*TU-C** *x*DSL Transmission Unit—central office. A hardware device that supports *x*DSL communication and that is placed in the CO. The *x*TU-C has a matching unit on the subscriber premise in the form of an *x*TU-R. The two units, in combination, support a high data rate over UTP copper cable local loops. Examples of *x*TU-Cs are ATU-C, ITU-C, STU-C, and SHTU-C.

***x*TU-R** *x*DSL Transmission Unit—remote. A hardware device that supports *x*DSL communication and that is placed in the customer's premise. The *x*TU-R has a matching unit in the carrier's CO in the form of an *x*TU-C. The two units, in combination, support a high data rate over UTP copper cable local loops. Examples of *x*TU-Rs are ATU-R, ITU-R, STU-R, and SHTU-R.

A

B

C

F

G

M

N

O

R

S

X