Cisco WAN Manager User's Guide

Release 10.5
October 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

Customer Order Number: DOC-7812945=
Text Part Number: 78-12945-02

Cisco WAN Manager User's Guide, Release 10.5

CONTENTS

FIGURES

Preface

The *Cisco WAN Manager User's Guide* describes how to use the Cisco WAN Manager Release 10 software.

Audience

This guide is designed for system administrators and users who are responsible for the operation of the Cisco WAN Manager application.

Organization

The major sections of this document are as follows:

Table 1 Cisco WAN Manager User's Guide Organization

Chapter Title	Description
Chapter 1, Cisco WAN Manager Overview	Provides an overview of the CiscoWAN Manager (CWM) product.
Chapter 2, Starting and Stopping Cisco WAN Manager	Describes how to start and stop CWM, using the main menu and using the CWM desktop.
Chapter 3, Network Topology	Describes the CWM Network Topology.
Chapter 4, Connection Manager	Describes how to use the CWM Connection Manager application and describes Connection Types and Service Types.
Chapter 5, Network Browser	Describes how to use the CWM Network Browser.
Chapter 6, Security Manager	Describes how to use the CWM Security Manager application.
Chapter 7, Service Class Template Manager	Describes how to use the CWM Service Class Template application.
Chapter 8, Statistics Collection Manager	Describes how to use the CWM Statistics Collection Manager application.
Chapter 9, Summary Report and Wingz	Describes the CWM Summary Report application and the Wingz Report application.
Chapter 10, Network Configurator	Describes how to use the CWM Network Configurator application.

Table 1 Cisco WAN Manager User's Guide Organization (continued)

Chapter Title	Description
Chapter 11, CWM to CWM Communications	Describes the implementation of communications between two or more CWM workstations.
Chapter 12, Downloading Software and Firmware	Describes downloading software and firmware.
Chapter 13, Saving and Restoring Node Configurations	Describes the save and restore configuration node commands.
Appendix A, Internet Connectivity	Describes CWM Internet connectivity.
Appendix B, Networking	Describes Networking with CWM.

Related Documentation

The following Cisco publications contain additional information related to the operation of this product and associated equipment in a Cisco WAN switching network.

Cisco WAN Manager Release 10.5 Documentation

The product documentation for the Cisco WAN Manager (CWM) network management system for Release 10.5 is listed in Table 2.

Table 2 Cisco WAN Manager Release 10.5 Documentation

Title	Description
Cisco WAN Manager Installation Guide for Solaris, Release 10.5 DOC-7812948=	Provides procedures for installing Release 10 of the CWM network management system and Release 5.3 of CiscoView.
Cisco WAN Manager User's Guide, Release 10.5 DOC-7812945=	Describes how to use the CWM Release 10 software which consists of user applications and tools for network management, connection management, network configuration, statistics collection, and security management.
Cisco WAN Manager SNMP Service Agent, Release 10.5 DOC-7812947=	Provides information about the CWM Simple Network Management Protocol Service Agent, an optional adjunct to CWM used for managing Cisco WAN switches using SNMP.
Cisco WAN Manager Database Interface Guide, Release 10.5 DOC-7812944=	Provides information about accessing the CWM Informix OnLine database that is used to store information about the network elements.

Table 3 WAN CiscoView Release 10 Documentation

Title	Description
WAN CiscoView Release 3 for the MGX 8850 Edge Switch, Release 1 DOC-7811242=	Provides instructions for using this network management software application that allows you to perform minor configuration and troubleshooting tasks.
WAN CiscoView Release 3 for the MGX 8250 Edge Concentrator, Release 1 DOC-7811241=	Provides instructions for using this network management software application that allows you to perform minor configuration and troubleshooting tasks.
WAN CiscoView Release 3 for the MGX 8230 Multiservice Gateway, Release 1 DOC-7810926=	Provides instructions for using this network management software application that allows you to perform minor configuration and troubleshooting tasks.

Cisco MGX 8850 Release 2.1 Documentation

The product documentation for the installation and operation of the MGX 8850 Release 2.1 switch is listed in Table 4.

Table 4 Cisco MGX 8850 Switch Release 2.1 Documentation

Title	Description
Cisco MGX 8850 Routing Switch Hardware Installation Guide, Release 2.1 DOC-7812561=	Describes how to install the MGX 8850 routing switch. It explains what the switch does, and covers site preparation, grounding, safety, card installation, and cabling.
Cisco MGX 8850 and MGX 8950 Switch Command Reference, Release 2.1 DOC-7812563=	Describes how to use the commands that are available in the CLI[1]of the MGX 8850 and MGX 8950 switches.
Cisco MGX 8850 and MGX 8950 Switch Software Configuration Guide, Release 2.1 DOC-7812551=	Describes how to configure the MGX 8850 and the MGX 8950 switches to operate as ATM edge and core switches. This guide also provides some operation and maintenance procedures.
Cisco MGX 8850 and MGX 8950 SNMP Reference, Release 2.1 DOC-7812562=	Provides information on all supported MIB[2]objects, support restrictions, traps, and alarms for the AXSM, PXM45, and RPM. PNNI is also supported.
Cisco MGX and SES PNNI Network Planning Guide DOC-7813543=	Provides guidelines for planning a PNNI network that uses the MGX 8850 and the MGX 8950 switches and the BPX 8600 switches. When connected to a PNNI network, each BPX 8600 series switch requires a Service Expansion Shelf (SES) for PNNI route processing.
Cisco MGX Route Processor Module Installation and Configuration Guide, Release 2.1 DOC-7812510=	Describes how to install and configure the MGX Route Processor Module (RPM-PR) in the MGX 8850 and MGX 8950 Release 2.1 switch. Also provides site preparation, troubleshooting, maintenance, cable and connector specifications, and basic IOS configuration information.

1. CLI = command line interface

2. MIB = Management Information Base

Cisco MGX 8950 Release 2.1 Documentation

The product documentation for the installation and operation of the MGX 8950 Release 2.1 switch is listed in Table 5.

Table 5 Cisco MGX 8950 Switch Release 2.1 Documentation

Title	Description
Cisco MGX 8950 Switch Hardware Installation Guide, Release 2.1 DOC-7812564=	Describes how to install the MGX 8950 core switch. It explains what the switch does, and covers site preparation, grounding, safety, card installation, and cabling.
Cisco MGX 8850 and MGX 8950 Switch Command Reference, Release 2.1 DOC-7812563=	Describes how to use the commands that are available in the CLI of the MGX 8850 and MGX 8950 switches.
Cisco MGX 8850 and MGX 8950 SNMP Reference, Release 2.1 DOC-7812562=	Provides information on all supported MIB objects, support restrictions, traps, and alarms for the AXSM, PXM45, and RPM. PNNI is also supported.
Cisco MGX and SES PNNI Network Planning Guide DOC-7813543=	Provides guidelines for planning a PNNI network that uses the MGX 8850 and the MGX 8950 switches and the BPX 8600 switches. When connected to a PNNI network, each BPX 8600 series switch requires a SES[1] for PNNI route processing.
Cisco MGX Route Processor Module Installation and Configuration Guide, Release 2.1 DOC-7812510=	Describes how to install and configure the MGX Route Processor Module (RPM-PR) in the MGX 8850 and MGX 8950 Release 2.1 switch. Also provides site preparation, troubleshooting, maintenance, cable and connector specifications, and basic IOS configuration information.

1. SES = Service Expansion Shelf

SES PNNI Release 1.1 Documentation

The product documentation that contains information for the understanding, the installation, and the operation of the Service Expansion Shelf (SES) PNNI Controller is listed in Table 6.

Table 6 SES PNNI Controller Release 1.1 Documentation

Title	Description
Cisco SES PNNI Controller Software Configuration Guide, Release 1.1 DOC-7813539=	Describes how to configure, operate, and maintain the SES PNNI Controller.

Table 6 SES PNNI Controller Release 1.1 Documentation (continued)

Title	Description
Cisco SES PNNI Controller Software Command Reference, Release 1.1 DOC-7813541=	Provides a description of the commands used to configure and operate the SES PNNI Controller.
Cisco MGX and SES PNNI Network Planning Guide DOC-7813543=	Provides guidelines for planning a PNNI network that uses the MGX 8850 and the MGX 8950 switches and the BPX 8600 switches. When connected to a PNNI network, each BPX 8600 series switch requires a SES for PNNI route processing.

Cisco WAN Switching Software, Release 9.3 Documentation

The product documentation for the installation and operation of the Cisco WAN Switching Software Release 9.3 is listed in Table 7.

Table 7 Cisco WAN Switching Release 9.3 Documentation

Title	Description
Cisco BPX 8600 Series Installation and Configuration, Release 9.3.30 DOC-7812907=	Provides a general description and technical details of the BPX broadband switch.
Cisco WAN Switching Command Reference, Release 9.3.30 DOC-7812906=	Provides detailed information on the general command line interface commands.
Cisco IGX 8400 Series Installation Guide, Release 9.3.30 OL-1165-01 (online only)	Provides hardware installation and basic configuration information for IGX 8400 Series switches running Switch Software Release 9.3.30 or earlier.
Cisco IGX 8400 Series Provisioning Guide, Release 9.3.30 OL-1166-01 (online only)	Provides information for configuration and provisioning of selected services for the IGX 8400 Series switches running Switch Software Release 9.3.30 or earlier.
Cisco IGX 8400 Series Regulatory Compliance and Safety Information DOC-7813227=	Provides regulatory compliance, product warnings, and safety recommendations for the IGX 8400 Series switch.

MGX 8850 Multiservice Switch, Release 1.1.40 Documentation

The product documentation that contains information for the installation and operation of the MGX 8850 Multiservice Switch is listed in Table 8.

Table 8 MGX 8850 Multiservice Gateway Documentation

Title	Description
Cisco MGX 8850 Multiservice Switch Installation and Configuration, Release 1.1.3 DOC-7811223=	Provides installation instructions for the MGX 8850 multiservice switch.
Cisco MGX 8800 Series Switch Command Reference, Release 1.1.3. DOC-7811210=	Provides detailed information on the general command line for the MGX 8850 switch.
Cisco MGX 8800 Series Switch System Error Messages, Release 1.1.3 DOC-7811240=	Provides error message descriptions and recovery procedures.
Cisco MGX 8850 Multiservice Switch Overview, Release 1.1.3 *OL-1154-01 (online only)*	Provides a technical description of the system components and functionary of the MGX 8850 multiservice switch from a technical perspective.
Cisco MGX Route Processor Module Installation and Configuration Guide, Release 1.1 DOC-7812278=	Describes how to install and configure the MGX Route Processor Module (RPM/B and RPM-PR) in the MGX 8850, MGX 8250, and MGX 8230 Release 1 switch. Also provides site preparation, troubleshooting, maintenance, cable and connector specifications, and basic IOS configuration information.
1.1.40 Version Software Release Notes Cisco WAN MGX 8850, MGX 8230, and MGX 8250 Switches DOC-7813594=	Provides new feature, upgrade, and compatibility information, as well as known and resolved anomalies.

MGX 8250 Edge Concentrator, Release 1.1.40 Documentation

The documentation that contains information for the installation and operation of the MGX 8250 Edge Concentrator is listed in Table 9.

Table 9 MGX 8250 Multiservice Gateway Documentation

Title	Description
Cisco MGX 8250 Edge Concentrator *Installation and Configuration, Release 1.1.3* DOC-7811217=	Provides installation instructions for the MGX 8250 Edge Concentrator.
Cisco MGX 8250 Multiservice Gateway Command Reference, Release 1.1.3 DOC-7811212=	Provides detailed information on the general command line interface commands.
Cisco MGX 8250 Multiservice Gateway Error Messages, Release 1.1.3 DOC-7811216=	Provides error message descriptions and recovery procedures.
Cisco MGX 8250 Edge Concentrator Overview, Release 1.1.3 DOC-7811576=	Describes the system components and functionality of the MGX 8250 edge concentrator from a technical perspective.

Table 9 MGX 8250 Multiservice Gateway Documentation (continued)

Title	Description
Cisco MGX Route Processor Module Installation and Configuration Guide, Release 1.1 DOC-7812278=	Describes how to install and configure the MGX Route Processor Module (RPM/B and RPM-PR) in the MGX 8850, MGX 8250, and MGX 8230 Release 1 switch. Also provides site preparation, troubleshooting, maintenance, cable and connector specifications, and basic IOS configuration information.
1.1.40 Version Software Release Notes Cisco WAN MGX 8850, MGX 8230, and MGX 8250 Switches DOC-7813594=	Provides new feature, upgrade, and compatibility information, as well as known and resolved anomalies.

MGX 8230 Multiservice Gateway, Release 1.1.40 Documentation

The documentation that contains information for the installation and operation of the MGX 8230 Edge Concentrator is listed in Table 10.

Table 10 MGX 8230 Multiservice Gateway Documentation

Title	Description
Cisco MGX 8230 Edge Concentrator Installation and Configuration, Release 1.1.3 DOC-7811215=	Provides installation instructions for the MGX 8230 Edge Concentrator.
Cisco MGX 8230 Multiservice Gateway Command Reference, Release 1.1.3 DOC-7811211=	Provides detailed information on the general command line interface commands.
Cisco MGX 8230 Multiservice Gateway Error Messages, Release 1.1.3 DOC-78112113=	Provides error message descriptions and recovery procedures.
Cisco MGX 8230 Edge Concentrator Overview, Release 1.1.3 DOC-7812899=	Provides a technical description of the system components and functionary of the MGX 8250 edge concentrator from a technical perspective.
Cisco MGX Route Processor Module Installation and Configuration Guide, Release 1.1 DOC-7812278=	Describes how to install and configure the MGX Route Processor Module (RPM/B and RPM-PR) in the MGX 8850, MGX 8250, and MGX 8230 Release 1 switch. Also provides site preparation, troubleshooting, maintenance, cable and connector specifications, and basic IOS configuration information.
1.1.40 Version Software Release Notes Cisco WAN MGX 8850, MGX 8230, and MGX 8250 Switches DOC-7813594=	Provides new feature, upgrade, and compatibility information, as well as known and resolved anomalies.

Document Conventions

This document uses the following conventions and terminology:

- pointer—indicates where the mouse action is to occur
- select—push and hold the left mouse button
- release—let up on a mouse button to initiate an action
- click—select and release a mouse button without moving the pointer
- double-click—click a mouse button twice quickly without moving the pointer
- drag—move the pointer by sliding the mouse with one or more buttons selected

CWM software supports a three-button mouse. The buttons have the following configurations:

- left button—selects objects and activates controls
- middle button—adjusts a selected group of objects, adds, or deselects a part of the group
- right button—displays and selects options from menus

Users can customize these buttons in an alternative manner.

In situations that allow the user to select more than one item from a list simultaneously, the following actions are supported:

- To select a single item in a list, click on the entry. To deselect a single item, click a second time on the previously selected entry.
- To select a contiguous block of items, click on the first entry; without releasing the mouse button, drag to the last desired entry and release. A subsequent click anywhere on the screen deselects all previous selections.
- To add an item to a selected group, press **Shift** and click on the entry at the end of the group to be added.
- To add a non-contiguous entry to the selection group, press **Ctrl** and click on the entry.

The following elements are in **boldface**:

- menu names
- buttons
- drop-down lists
- keyboard names

Words and characters that are displayed in terminal sessions and on-screen are printed in `screen font`.

When set off from the main text, words and characters that the user enters are printed in **boldface screen font**.

Word or character strings enclosed in angle brackets < > indicate that users substitute their own character string for the example presented in the text. When referenced in body text, the word is in **boldface** (not `screen font`). See the following examples:

- login: **`root`**—Enter the string **`root`** at the login prompt.
- password: <*rootpassword*>—Enter the password in place of the character string <*rootpassword*>.

Command descriptions use the following conventions:

- Commands and keywords are in **boldface**.
- Arguments that require values are in *italic*.

- Required command arguments are inside angle brackets < >.
- Optional command arguments are in square brackets [ ].
- Alternative keywords are separated by vertical bars (|).

Examples use the following conventions:

- Terminal sessions and system displays are in `screen font`.
- Information users enter is in **boldface screen font**.
- Non-printing characters, such as passwords, are in angle brackets < >.
- Default responses to system prompts are in square brackets [ ].

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 CD-ROM package, which ships 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 as an annual subscription.

Ordering Documentation

Cisco documentation is available 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

- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:

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

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

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can submit technical comments electronically. Click **Feedback** in the toolbar and select **Documentation**. After you complete the form, click **Submit** to send it to Cisco.

You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

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

We appreciate your comments.

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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

http://www.cisco.com

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

http://www.cisco.com/tac

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1(P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

Cisco WAN Manager Overview

Cisco WAN Manager (CWM), a suite of WAN multiservice management applications, provides powerful fault, configuration, and performance management functionality for WAN multiservice switches. CWM also provides robust statistics collection, storing the information in an Informix SQL database and allowing simple integration of this data into existing network management and operations systems.

Element and network management functions are provided by the CWM system, which can manage Cisco BPX® 8600 and Cisco IGX™ 8400 series wide-area switches, the Cisco BPX SES PNNI Controller, and Cisco MGX™ 8220, Cisco MGX™ 8230, Cisco MGX™ 8250, and both Release 1 and Release 2 Cisco MGX™ 8850 devices seamlessly. CWM provides open interfaces for higher level service management systems.

The CWM desktop graphical user interface (GUI) provides the following applications that are found under the **Apps** pull down menu of the CWM Topology Main Window:

- Connection Manager
- Network Browser
- Service Class Template Manager
- Statistics Collection Manager
- Security Manager
- Summary Report
- Wingz Report
- Cisco View

CWM provides these functions in an open management environment. CWM runs on Release 2.7 of Solaris and integrates with Release 6.10 of HP OpenView.

CWM Release 10 Applications

Connection Manager

The Connection Manager provides the network manager the ability to add, modify, and delete end-to-end connections. The Connection Manager provides a series of forms-based screens to add, modify, or delete connections. You select the desired connection end-points and configure the connection type and class

of service. The end-to-end connection is automatically established without requiring configuration of the network on a switch-by-switch basis. In addition, each connection's status can be viewed from one endpoint to the other.

Connection management is one of the most challenging issues in ATM network management. ATM networks support so many connections that it can become impossible to administer and manage them. The Connection Service MIB provides integrated automated provisioning of connections based on quality of service parameters, such as the type of connection being made, available bandwidth, and the current state of the network.

The Connection Service MIB provides a standard SNMP interface for the WAN ATM network at the service level. Service providers who are responsible for managing the entire shared network can use this interface to integrate with automated Operations Support Systems (OSS) provisioning systems, and also to provide Customer Network Management (CNM) views and control capabilities on a per-connection basis.

Network Browser

The Network Browser application provides a hierarchical representation of network information in a table format. Each network element managed by Cisco WAN Manager (CWM) has its own attributes and fits in the network's physical or logical hierarchy. In Release 10 of CWM, the Network Browser presents the network elements that are discovered, managed, and controlled in a hierarchical view for all networks populated in the network table by CWM processes.

The Network Browser displays the network elements in a hierarchical format based on either a physical or logical relationship among the various network elements. Networks are displayed at the root level of the component tree, and nodes and trunks are displayed beneath the networks in a parent/child relationship.

The Network Browser also displays informational messages in a multi-line text display. Other types of messages can be displayed in response to user actions.

Service Class Template Manager

The Service Class Template (SCT) application is a new Java-based application for Release 10 of CWM that allows for creating SCT files which can then be loaded to nodes, and can be associated with interfaces on cards within these nodes. This application is launched from the CWM desktop and allows users and network operators to configure AXSM, AXSM-E, and RPM cards, using the Service Class Template feature. Specifically, users or network operators are able to use the SCT application to create, modify, delete, load, and associate SCT files to AXSM cards and ports.

Statistics Collection Manager

The Statistics Collection Manager (SCM) for Release 10 of CWM is a new stand alone collector that allows a separate SCM collection server in both installation and statistics collection. This new feature allows you to control and manage statistics collection through a stand alone application. The Statistics Controller Server, Statistics Collection Server, and Statistics Parser Server provide statistics applicable to the different cards and nodes.

The Statistics Collection Manager (SCM) provides a forms-based interface to establish and modify statistic collection policies for the network. You can configure statistic collection policies such as which statistics to collect, and collection interval periods for a node, port, or private virtual circuit (PVC). SCM provides extensive error handling and logging capabilities that enable reliable collection of statistics for performance or billing applications.

Security Manager

The Security Manager (SM) application is a new Java-based application for Release 10 of CWM that provides controlled access to multiple users of CWM based on the unique user ID and password. You can use Security Management to provide individuals access privileges to perform specific tasks such as viewing topology or establishing and managing connections. Without the required access privileges, unauthorized users cannot perform any network management functions.

Wingz Report and Summary Report

CWM Statistics Reports are generated through a graphical reporting package based on the Informix **Wingz Report** application. CWM also provides node utilization reports not based on Wingz. These reports are obtained through the **Summary Report** application. Both the Wingz Report and the Summary Report applications provide a point-and-click graphical user interface to generate reports based on information collected by the Statistics Agents. For each report, the user identifies certain criteria, such as network object, type of statistics, granularity, report interval, and graphical format, depending on the Report application selected. For the Wingz Report, the report agent queries the Informix database and generates a report in the desired format, such as line, bar, 3D, or tabular chart. Scalability of statistic collection is an important differentiator of CWM.

Cisco View

WAN Cisco View is a JAVA-based device management software GUI application that allows you to:

- Display a graphical representation of the network device
- Display configuration and performance information
- Perform minor configuration tasks
- Perform minor troubleshooting tasks

WAN Cisco View supports card, line, and port configuration on the MGX 8220, 8230, 8250, Release 1 and 2 of the MGX 8850, IGX 8400 series, BPX 8600 series, and BPX SES PNNI Controller.

Additional CWM Release 10 Applications and Features

Configuration Save and Restore

The **ConfigSave and Restore** feature can be found under the **Tools** pull down menu of the CWM Topology Main Window. This feature enables you to save a snapshot of the entire network's configuration on CWM. In a disaster recovery scenario, you can selectively restore a single node's configuration, or restore the configuration of the entire network on a node by node basis. This feature significantly reduces time to recover in the unlikely event of a catastrophic failure. You can also use the Save and Restore feature to restore a previous configuration after making a series of incorrect or temporary changes.

Network Configurator

The Network Configurator is a new Java-based application for Release 10 of CWM that enables users to add new nodes, or modify or delete existing nodes. It is also used to provide descriptor information, node name, and IP address information for the nodes in your network. **The Network Configurator is started by entering runConfigurator** <*machine name*> **<*login*>** <*password*> on a shell's command line, where Cisco WAN Manager Release 10 is installed**.** The Network Configurator main window appears, allowing the user to add, delete, and modify nodes.

CWM to CWM Communications

Release 10 of Cisco WAN Manager has been designed to enable multiple CWM workstations to manage a network with improved network synchronization and scalability. Due to the size and growth of networks, it is faster to retrieve initial network information from another CWM workstation that is already running and synchronized with the network.

A new CWM feature now enables users to continue the provisioning of network data, even when communications between a Primary CWM and Secondary CWM have been interrupted. If for any reason the communications between CWM servers are interrupted, user data provisioning will be suspended on the Secondary CWM, but user data provisioning will continue on the Primary CWM. During that time, the provisioning of user data and monitoring of the network are not impacted. This is called the Degraded Mode of Operation, and is discussed in Chapter 11, CWM-CWM Communications.

Release 10 of CWM uses an industry standard CORBA architecture to implement the communications between two or more CWM workstations. The architecture uses a server-client structure for communications between the CWM server and client processes.

Access to IGX, BPX, and MGX Networks

IGX, BPX, and MGX switches provide an Ethernet 802.3 AUI LAN interface to CWM for network management control and information. An entire network can be managed through an Ethernet connection on a single WAN switch or through multiple Ethernet interfaces distributed throughout the network. Cisco WAN switches use TCP/IP over Ethernet to communicate between CWM network management workstations and the WAN switch. Telnet support is also available to enable LAN-based workstations access to the IGX, BPX, or MGX management interface.

Graceful Software and Firmware Download and Upgrades

Software and Firmware downloading of all operating system and firmware code is fully supported by BPX, IGX, MGX, and CWM. Software and firmware upgrades are performed by loading new code from either a CWM workstation via TCP/IP, a new NPM module, or via dial in from Cisco's Technical Assistance Center (TAC). New software and firmware are downloaded throughout the network utilizing inter-nodal trunks. New code is loaded into the standby NPM card for initiation at a specified time. This new code can be uploaded to all other IGXs in-band through the ATM fabric connecting the switches.

Firmware upgrades for a specific function module are performed by first loading the new firmware code into the NPM. Then a command is issued to *burn* the function module with the new firmware revision. This may take up to ten minutes, during which time the function module is out of service. Software upgrades are conducted in background, and then activated network wide. The duration of a software activation is 10 seconds per node on a rolling basis. Configuration translation software is provided with software upgrades to automatically migrate existing configuration information into new software releases.

Simultaneous upgrades to multiple devices is supported via background loading of new code and simultaneous switching to the new code.

During all software and firmware upgrades the current configuration is retained. The conversion is automatic and performed by the new software release. If a software upgrade is faulty a single command can return the entire network to the previous version software and configuration in ten seconds.

Performance Management

The CWM TFTP statistics collection facility offers extensive usage and error collection. A wide range of statistics are available at the port and virtual channel level to support operations and maintenance, customer network management and usage-based billing. Historical statistical information is stored in the CWM Informix database. The open SQL interface architecture then provides users with direct access to the information stored in the Informix relational database. CWM addresses historical information via the SQL architecture because of the large volume of information present in the database and the inefficiencies involved in retrieving it via SNMP.

- Connection Statistics
- Circuit Line Statistics
- Packet Line Statistics
- Frame Relay Port Statistics
- ATM Statistics
- Physical Layer Statistics
- ATM Layer Statistics

Open Management

CWM provides seamless element and network management for the complete Cisco WAN multiservice switching product portfolio, including BPX, MGX, and IGX. The distributed intelligent architecture enables each network element to collect comprehensive performance and utilization statistics. Each node stores these statistics in a file which is then transferred to CWM, where it is stored in the SQL database.

Operating within the HP OpenView multi-vendor management environments, CWM supports a suite of open interfaces for access to management information including:

- Standard management integration protocols interfaces, including SNMP
- SQL access to the Informix relational traffic database
- X-terminal access for multiple operators into CWM management agents
- Craft interface for terminals and simple tools

WAN multiservice management can be integrated within the multi-vendor environment using third party applications in conjunction with the CWM application. Otherwise, integration management interfaces and software tools can achieve fault, configuration, performance and security management through the open management interfaces.

Event Manager

Network faults are integrated with the HP OpenView Event Browser to enable management of heterogeneous, multi-vendor network environments. Through the Event Browser the events can be filtered by a combination of event type, source, message string, time received, and severity, grouped into categories based on event severity, or acted-on through custom-defined operator actions. Different actions can be configured on a per-node basis such that the same type of event from different sources cause different automatic actions.

Network Topology

The Cisco WAN network topology is automatically discovered and presented through topology map windows. Network element and trunk status are represented by icon color changes dynamically. Custom background images can be associated with each network map to provide a user-defined view of the network.

Starting and Stopping Cisco WAN Manager

This chapter provides information about starting and stopping Cisco WAN Manager (CWM), using the CWM main menu, CWM in restricted access mode, and starting HP OpenView.

Starting Cisco WAN Manager

This section provides information about starting CWM. This section includes the following procedures:

- Starting CWM from a workstation for the first time
- Performing a warm start of CWM
- Performing a cold start of CWM

Note These procedures describe CWM startup from a workstation running the Sun Solaris operating system.

Starting CWM for the First Time

This section describes how to start CWM for the first time. This procedure is also used to start CWM from a workstation that has been powered off.

Step 1 Turn on power to any peripheral devices, such as external disk drives, tape drives, or monitors, then turn power on to the workstation.

Observe the messages that are displayed on the workstation as it boots up, and wait for the login prompt. While the Solaris OS is booting, the HPOV SNMP Agent, the HPOV background processes, and the Informix database are also started.

Step 2 At the Solaris login window, click on **Options > Session > CDE**.

Note This step is necessary only on the first login. If asked during the login process, select CDE again.

Step 3 Login to the workstation as user **svplus**.

Step 4 Left click the TTT icon to launch the Style Manager and perform the following steps to save system resources:

a. Click on Screen, Screen Saver, and Screen Lock Off.

b. Click on Backdrop, select GrayDk, then click Apply.

Step 5 Use the CDE Menu Bar to change to screens Two, Three, and Four, and select the same options for those screens. Return to screen One and close Style Manager when completed.

Step 6 Right click on the desktop and select **Programs** > **Terminal**.

Move this window to the upper-right corner of the screen.

Step 7 Right click on the desktop and select **Programs** > **Console**.

Reduce the height of this window so it displays at least five lines (to enable you to monitor system messages). Move the window so that it rests on the CDE Menu Bar and all icons are visible.

Note Do not use the Console window for any purpose other than monitoring system messages.

Step 8 Left click the TTT icon to launch the Style Manager, then select **Startup**, **Set Home Session...**, and click **OK**.

This saves your startup login preferences.

Note In a CDE environment, if a Home Session has not been set, any previously opened applications will run. If the console and terminal windows do not open under CDE, right click the mouse on an empty portion of the background and select **Programs** > **Console**, then select **Programs** > **Terminal**.

Step 9 In the terminal window, enter **CWM** to display the CWM main menu.

Note If the error message "Environment Variable DISPLAY not set" is displayed when you attempt to start the main menu and the display is not being xhosted to another workstation, enter the following: **setenv DISPLAY *machine_name*:0.0**

Step 10 Enter **1** to select the Start Core option and press **Return**.

Observe the messages that are displayed. Notice the gateway and stand alone nodes *socketed* messages to the IP-LAN addresses.

A Link0 down message may be displayed, followed by a Link0 up for each gateway node (if communication is established to the gateway node), then a group of Link1 up messages for all nodes, if everything is working correctly.

There will probably be several ILOG RT-Broker messages; disregard these messages and the EMSD dumping message, if it is displayed. This is normal operation. Also disregard any server EMDAEMON not registered messages.

Note Additional messages will be displayed for PNNI nodes.

After you see the Link 0, Link 1, and gateway node messages indicating the connections are up, continue to the next step. (If there is a problem with a Link connection, you will not see all connections come up.

Note Stand alone MGX 8850 switches do not use Link protocol and will not show up in these messages. Feeder MGX 8850 switches act like MGX 8220 switches and do not display Link 1 messages.

Step 11 Press **Return** to redisplay the main menu.

At this point, you can issue other main menu options to start the CWM desktop or the Statistics Manager.

Step 12 Enter **3** to launch the CWM Desktop.

Step 13 From the CWM Desktop, left click on the Statistic Collection Manager icon to launch the Statistics Manager application.

Minimize the Statistic Collection Manager window.

Step 14 Right click on the desktop and select **Programs** > **Terminal** to open another xterm window.

Step 15 In the new xterm window, enter **ovw &** to start the Openview application which opens the Openview graphical user interface (GUI) and the Event Manager.

The IP map contains HPOV's view of the attached IP network and the CWM map contains the CWM nodes which are displayed directly from CWM via the SvOvTopology daemon. Use the buttons in the Event Manager window to view desired event categories.

Performing a Warm Start of CWM

A warm start of CWM consists of stopping the application, then restarting it. A warm start of CWM can aid in overcoming some database inconsistencies, and more importantly, no data is lost. **When you perform a warm start of CWM, the application continues to use data in the existing Informix database**.

To perform a warm start of CWM, complete the following steps:

Step 1 From the CWM main menu, enter **2** to select the **Stop Core** option, then confirm that you want to stop core by responding **y** to the prompt.

It should take less than a minute for all of the processes and messages to end.

Step 2 Press Return to redisplay the CWM main menu.

Step 3 From the main menu, enter **1** to select the Start Core option.

Step 4 When the CWM main menu is displayed, enter **3** to launch the CWM Desktop.

Performing a Cold Start of CWM

You perform a cold start of CWM when you start the application with an empty database. A cold start is typically used following a CWM upgrade or if there were too many database inconsistencies within the network for a warm start recovery to be successful. You use the **create_db** command to build a new, empty database. The command **create_db destroys any existing data in the database including statistics and object comments**.

Cold start options include the following:

- coldstart -F
- coldstart
- coldstartSCM

- coldstartSCM -F

To perform a cold start of CWM, complete the following steps:

Step 1 At the CWM workstation, enter **CWM** to display the main menu.

Step 2 From the CWM main menu, enter **2** to select the **Stop Core** option, then confirm that you want to stop core by responding **y** to the prompt.

It might take several minutes for all of the processes and messages to end, depending upon the number of nodes in the network.

Step 3 Press Return to redisplay the CWM main menu.

Step 4 From the main menu, enter **x** to exit the CWM application.

Step 5 Enter **create_db**.

Dozens of messages will be displayed, starting with the message **dropping db**. Additional messages will indicate that tables are being created and procedures stored. The shell prompt will return in less than a minute.

Step 6 At the CWM workstation, enter **CWM** to redisplay the main menu.

Step 7 From the main menu, enter **1** to select the Start Core option.

Step 8 When the CWM main menu is displayed, enter **3** to launch the CWM Desktop.

Stopping Cisco WAN Manager

This section provides information about stopping CWM. This section includes the following procedures:

- Stopping the CWM application
- Stopping the CWM application and powering off the workstation

Stopping CWM

To stop the CWM application, complete the following steps:

Step 1 Close the HP Openview application (if it is running) by selecting **Map > Exit** from any Openview window and click **OK** when prompted to confirm the operation.

Step 2 Close the CWM Desktop by selecting **File > Exit** from the Desktop main window.

Step 3 If the Statistics Manager is running, select **File > Quit** and click **OK** when prompted to confirm the operation.

Step 4 Close any other CWM applications, such as Connection Manager, that might be currently running.

Step 5 From the CWM main menu, enter **2** to select the **Stop Core** option, then confirm that you want to stop core by responding **y** to the prompt.

It might take several minutes for all of the processes and messages to end, depending upon the number of nodes in the network.

Step 6 Press **Return** to redisplay the CWM main menu.

Step 7 From the main menu, enter **x** to exit the CWM application.

Stopping CWM and Powering Off the CWM Workstation

This section describes the proper method of stopping the CWM application to power down the workstation.

Step 1 In the CWM terminal window, switch to user **root**, and enter the following to halt the workstation:

sync; sync; halt

Instead of the **halt** command, you can use the **shutdown** command to broadcast a shutdown message to all logged-in users. Enter one of the following:

- # **sync; sync; shutdown -i 0 -g 0** (firmware)
- # **sync; sync; shutdown -i 5 -g 0** (power off)
- # **sync; sync; shutdown -i 6 -g 0** (reboot)

Note If you issue a **shutdown** command, the following step is unnecessary.

Step 2 At the OK prompt, enter the following to power down the workstation:

OK **power-off**

CWM Main Menu

Upon launching CWM, the **Main Menu** is displayed, enabling you to initiate and terminate the CWM core processes and to access the CWM Desktop window. You can also use the main menu to get the name of the current database.

To launch Cisco WAN Manager and display the main menu, open a C-shell window on the workstation where CWM has been installed, and complete the following steps:

Step 1 Log in as user **svplus** at the CWM workstation.

Step 2 Start CWM:

host% **CWM**

The CWM **Main Menu** is displayed as shown in Figure 2-1. To select any of the menu options, specify the number and press **Return**.

Step 3 From the CWM **Main Menu**, start the CWM Core process. Specify **1** at the prompt then press **Return** to initiate the **Start Core** option.

Figure 2-1 CWM Main Menu

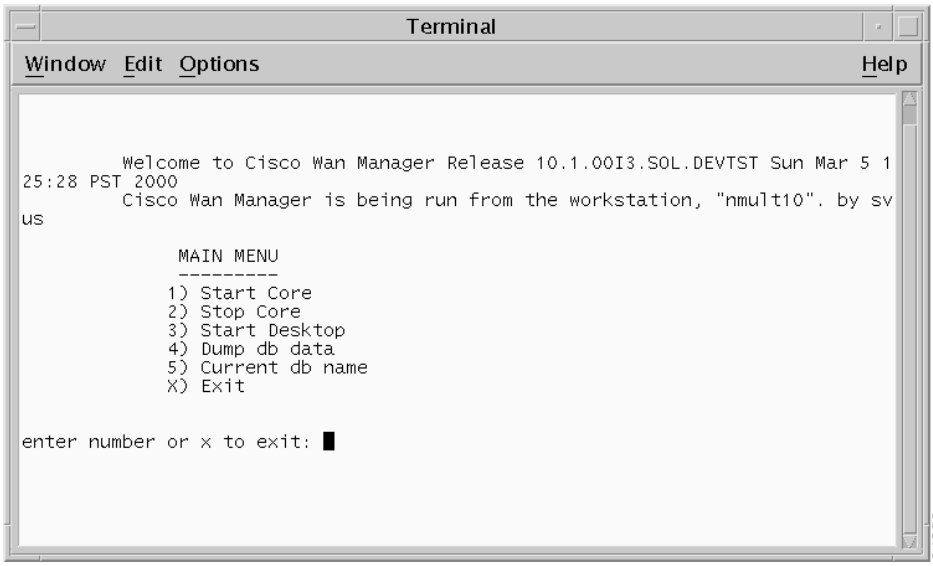


Table 2-1 lists the CWM main menu options

Table 2-1 CWM Main Menu Options

Menu Option	Descriptions
Start Core	Starts the CWM core and initiates CWM daemon processes
Stop Core	Stops the CWM daemon processes
Start Desktop	Displays the CWM desktop window
Dump db data	This option is no longer supported. For information on saving the data in the Informix database, refer tothe Cisco WAN Manager Database Interface Guide, Release 10.
Current db name	Displays the name of the database currently loaded in CWM
Exit	Exits CWM without shutting down the CWM core processes

Restricted Access Users

For Release 10 of Cisco WAN Manager , a new CWM desktop application, CWM Administration, manages user security. CWM Administration allows restricted access logins to enable users to perform tasks based on detailed access privileges. The user **svplus** still exists and should be used by experienced and trusted system administrators.

Note In earlier releases of Cisco StrataView Plus (release 9.1 and below), the **svplus-r** account was created when the application was installed on the workstation. The svplus-r account has been removed from CWM starting with release 9.2.

CWM Administration provides controlled access through the user's Unix userID and password by customizing user-access profiles. The user access profiles comprise a list of Access Privileges for users for a specific function including:

- ConMgr
- NW Topology
- Image Download
- Node Resync

For each action, a user may be given privileges to read, create, modify or delete functions, or a user may have all privileges to manage all or some actions.

Note As in previous releases, only user **svplus** can start and stop the CWM core processes.

Starting HP OpenView

This section describes how to start the HP OpenView application. To start the HP OpenView application, complete the following steps:

Step 1 From one of the C-shell windows, launch CWM and start the core processes.

Step 2 In the second window, invoke the HP OpenView application by entering the following at a command line prompt:

ovw &

Step 3 Several windows are displayed including warnings, Event Categories, and status updates. Eventually the Root window is displayed.

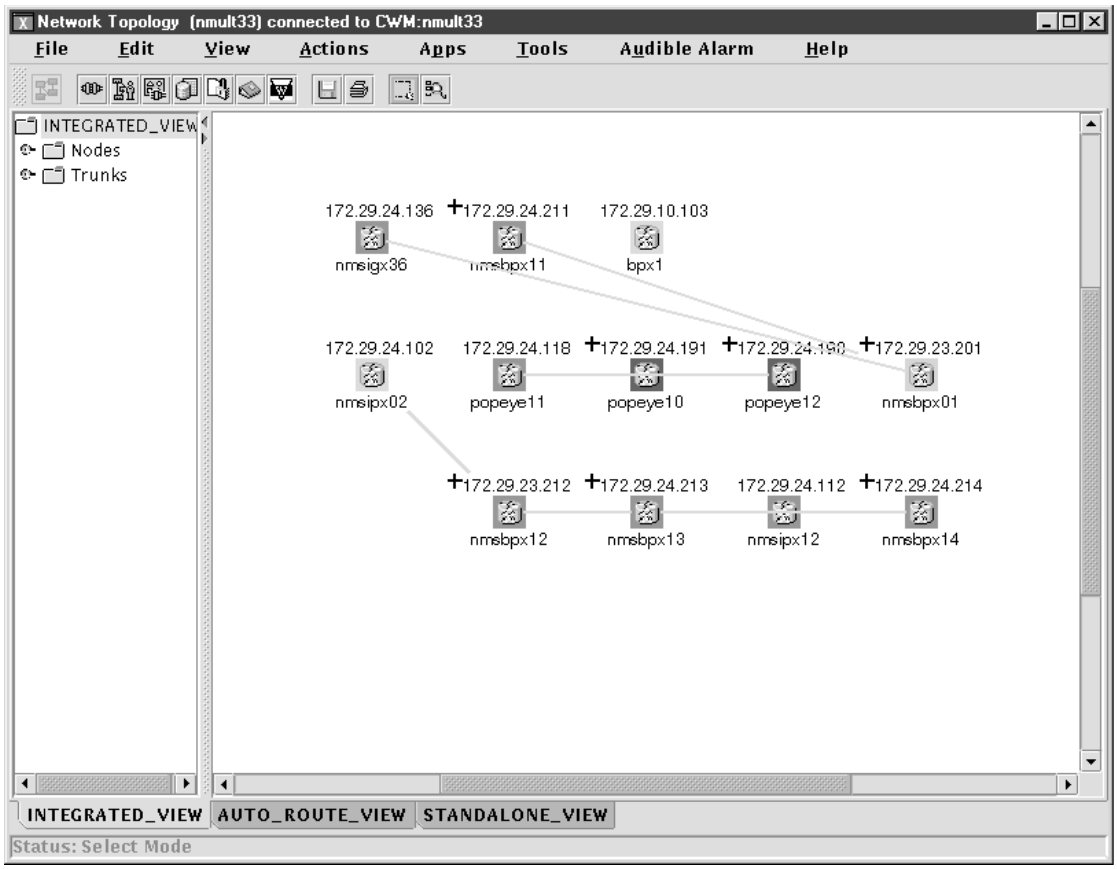
Step 4 Double-click on the **CWM Network** icon to display the CWM Network Topology window.

From the pull-down menus, you can launch all of the CWM features. Many menu items are disabled until an appropriate element is selected, such as a node in the topology.

The CWM Desktop Window

The CWM Desktop window (Figure 2-2) provides icon buttons that correspond to the principal CWM applications. You click on a particular icon to launch the corresponding application you need for network management, monitoring, report generation, and administration tasks. All the CWM applications are described in subsequent chapters in this book.

Figure 2-2 CWM Desktop Window



CWM Desktop Applications

The following section describes the CWM Desktop applications.

Connection Manager

Select this application to create end-to-end connections or Permanent Virtual circuits (PVCs). The Connection Manager application is described in detail in Chapter 4, “Connection Manager”.

Network Browser

Select this application to view a hierarchical representation of network information in a table format. The Network Browser application is described in detail in Chapter 5, “Network Browser”.

Service Class Template Manager

Select this application to create SCT files which can then be loaded to nodes, and can be associated with interfaces on cards within these nodes. The Service Class Template application is described in detail in Chapter 7, “Service Class Template Manager”.

Statistic Collection Manager

Select this application to control and manage statistics collection. The Statistic Collection Manager application is described in detail in Chapter 8, “Statistic Collection Manager”.

Security Manager

Select this application to provide individuals access privileges to perform specific tasks such as viewing topology or establishing and managing connections. The Security Manager application is described in detail in Chapter 6, “Security Manager”.

Summary Report

Select this application to view the Summary Report application window which provides basic performance reports including historical statistics on connection traffic, connection traffic dropped, trunk traffic, and network resource capacity.

Wingz Report

Select this application to open the Wingz spreadsheet to view statistics retrieved from the Informix database.

Cisco View

Select this application in order to:

- Display a graphical representation of the network device
- Display configuration and performance information
- Perform minor configuration tasks
- Perform minor troubleshooting tasks

WAN Cisco View supports card, line, and port configuration on the MGX 8220, 8230, 8250, Release 1 and 2 of the MGX 8850, IGX 8400 series, BPX 8600 series, and BPX SES PNNI Controller.

Network Configurator

Select this application to add new nodes, or modify or delete existing nodes on your network. The Network Configurator application is described in detail in Chapter 10, “Network Configurator”.

Starting Additional CWM GUIs

Note To run multiple Cisco WAN Manager GUIs, you must have a multi-user Wingz license.

More than one workstation can run the CWM GUI simultaneously. To run an additional CWM GUI, complete the following steps:

Step 1 Log into a workstation other than the one running the CWM core processes.

Step 2 Enter the following command:

xhost +

This is not necessary if both workstations have the other in its **/etc/xhost** file as a “+.”

Step 3 Do a remote login to the CWM workstation.

rlogin -*l login_id hostname*

Note You can also use the **telnet** command to connect to the remote host.

Step 4 Set the DISPLAY environmental variable by entering the following:

setenv DISPLAY *ip_address***:0.0**

where *ip_address* is the IP address of the workstation from which you have issued the telnet command.

Step 5 Launch CWM by entering **CWM**, then select Start Desktop from the main menu.

Note CWM core processes running on a workstation can be stopped from any other workstation that is running a remote CWM session. For example, when you log into a workstation running the CWM core processes and select **Stop Core** (Option **2**), you are terminating the CWM core processes for not only yourself, but for all others using those CWM core processes. Therefore, you must be careful not to select the **Stop Core** option when you are through. Take care to close only the windows you have opened remotely, and at the CWM main menu, select **X** to exit the application.

Network Topology

The CWM Network Topology application is a Java-based application that is launched from the CWM desktop. The CWM topology subsystem has been updated in Release 10 of CWM to provide better modularity and greater scalability. New processes within the topology server handle different types of network discovery, and individual clients have a direct connection to the topology server for their respective topologies.

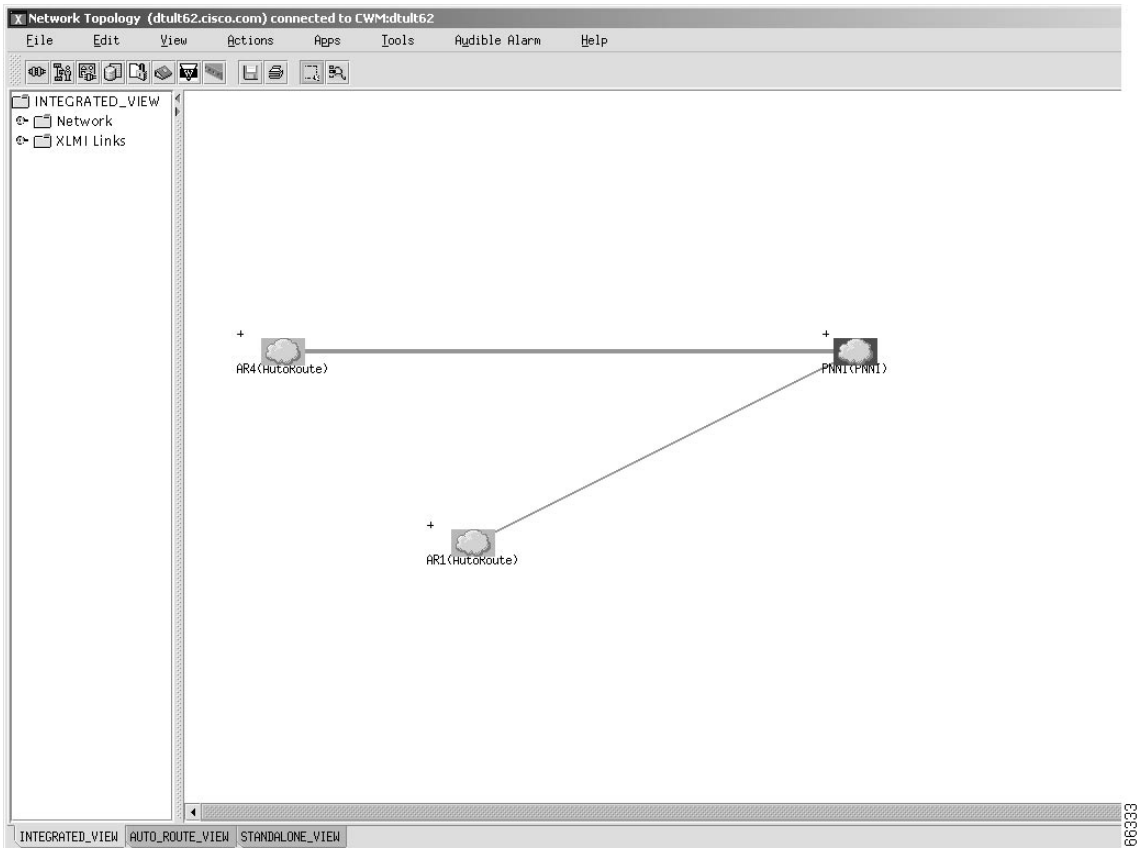
Release 10 of CWM has the additional benefit of easy access features that have been streamlined into the Network Topology, resulting in a more accessible and convenient way to navigate, discover and display the network.

Topology Main Window

Figure 3-1 shows the main window of the Network Topology which contains the following components:

- Title bar—displays the hostname of the CWM server (also known as the topology gateway) to which a given instance of network topology is connected.
- Menu bar—Provides available menu options for the network topology application.
- Tool bar—Contains the most frequently used actions in icon format. The tool bar can be modified to display vertically as well as horizontally, depending on your preference.
- Hierarchy tree and graph—Contain topology information in list or textual format (hierarchy tree) or in a graphical view. The hierarchy tree displays much more information that the graphical view. However, the graphical view more readily displays relationships, locations, and status of components.
- Tabs—Provide different views of the topology information based upon criteria such as discovery protocol. Each tab holds hierarchy tree and graph views. The vertical panel that separates these views can be moved to resize either the hierarchy tree or the graph view.
- Status bar—Displays any errors or informational messages as you attempt to perform various actions.

Figure 3-1 Network Topology Display



Title Bar

Displays the hostname of the CWM server.

Menu Bar

The network topology menu bar allows you to make a selection by pulling down a menu and clicking on a desired action. The following are available:

- File
- Edit
- View
- Actions
- Apps
- Tools
- Audible Alarm
- Help

Left click on the menu to view the available options. Scroll to the selected option and release the mouse button to select a menu item. Additionally, keyboard shortcuts (accelerators) and mnemonics are also provided to directly launch a menu selection.

The available menu options are discussed in detail later in this chapter.

Tool Bar

The network topology toolbar replaces the desktop of previous releases of CWM and Cisco StrataView Plus. The network topology toolbar provides icons that enable you to launch the more frequently used functions of CWM. The following CWM applications, (discussed in detail later in this chapter), can be launched by clicking on the appropriate icon:

- Connection Manager
- Network Browser
- Service Class Template Manager
- Statistics Collection Manager
- Security Manager
- Summary Reports
- Wingz Reports
- Cisco View

The following functions are also available on the network topology tool bar:

- Save
- Print
- Select
- Zoom

The network topology tool bar is a dockable tool bar. You can separate the toolbar from the network topology main window or position it vertically instead of horizontally. To separate the tool bar, left click the mouse in the tool bar position handler and drag the tool bar to the desktop location you prefer.

Hierarchy Tree and Graph

The Hierarchy tree and graph panels provide topology information in a list or textual format (hierarchy tree) or in a graphical view. The hierarchy tree displays much more information than the graphical view. However, the graphical view more readily displays relationships, locations, and status of components.

Network Topology Views

Tabs at the bottom of the Network Topology Main Window provide different views of the topology information based upon the type of view desired. Each tab holds hierarchy tree and graph views. The vertical panel that separates these views can be moved to resize either the hierarchy tree or the graph view. The three tabs are:

- Integrated_View
- Auto_Route_View

- Standalone_View

Status Bar

Displays any errors or informational messages as you attempt to perform various actions

Using the Network Topology Menus

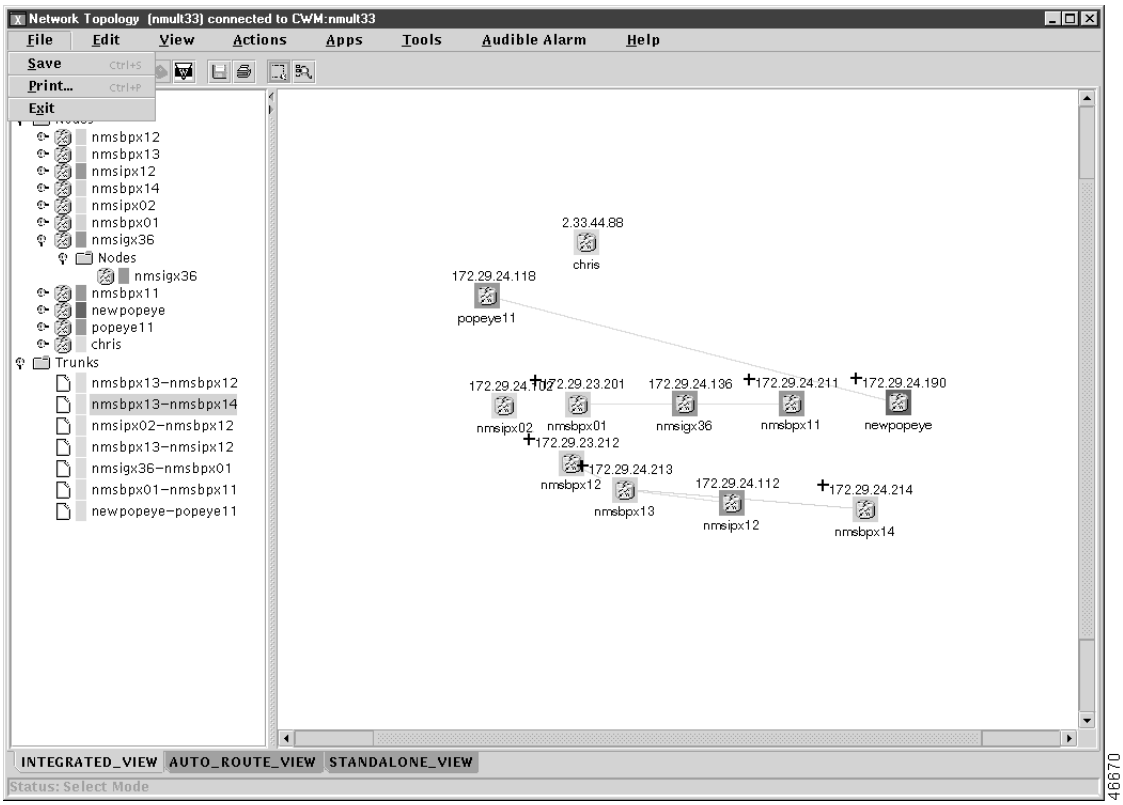
This section describes the functions provided via the network topology menus.

File Menu

The **File** menu, shown in Figure 3-2, the provides network topology application level operations.

Note The sequence to open the file menu is to press the Alt and F keys simultaneously.

Figure 3-2 File Menu Options



Save

The **Save** option saves the current positions of the nodes, trunks, and group information in all of the views.

Mnemonic	Accelerator
Alt + S	Ctrl + S

Print

The **Print** option prints the current view of the topology main window.

Mnemonic	Accelerator
Alt + P	Ctrl + P

Exit

The **Exit** option exits the network topology application and closes the main window.

Mnemonic	Accelerator
Alt + X	None available

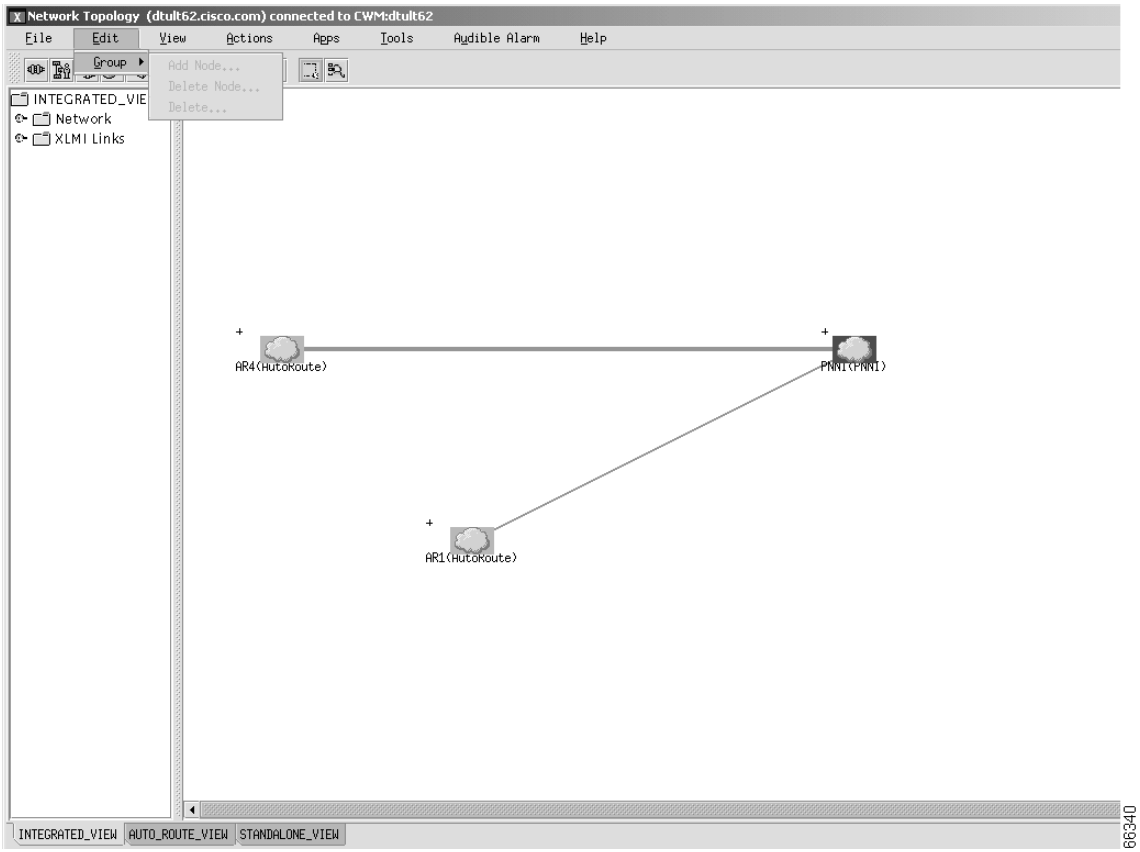
Note Closing the network topology application also removes your tool bar access to other CWM applications, unless you have detached the tool bar from the network topology GUI.

Edit Menu

The **Edit** menu, shown in Figure 3-3, provides editing access to network topology information using a **Group** submenu.

Note The mnemonic to open the file menu is to press the Alt and E keys simultaneously. There are no other mnemonics or shortcuts available for the edit menu options.

Figure 3-3 Edit Menu



Group

The **Group** submenu provides editing of network topology information through the following options:

Add Node

Selecting the **Add Node** option displays a dialog box into which you provide the required information for a node to be added to the network.

Delete Node

Selecting the **Delete Node** option displays a dialog box into which you provide the required information to delete a node from the network.

Delete

Selecting the **Delete** option displays a dialog box into which you provide the required information to delete a group of nodes from the network.

View Menu

The **View** menu provides the following options which directly change the current view of network topology:

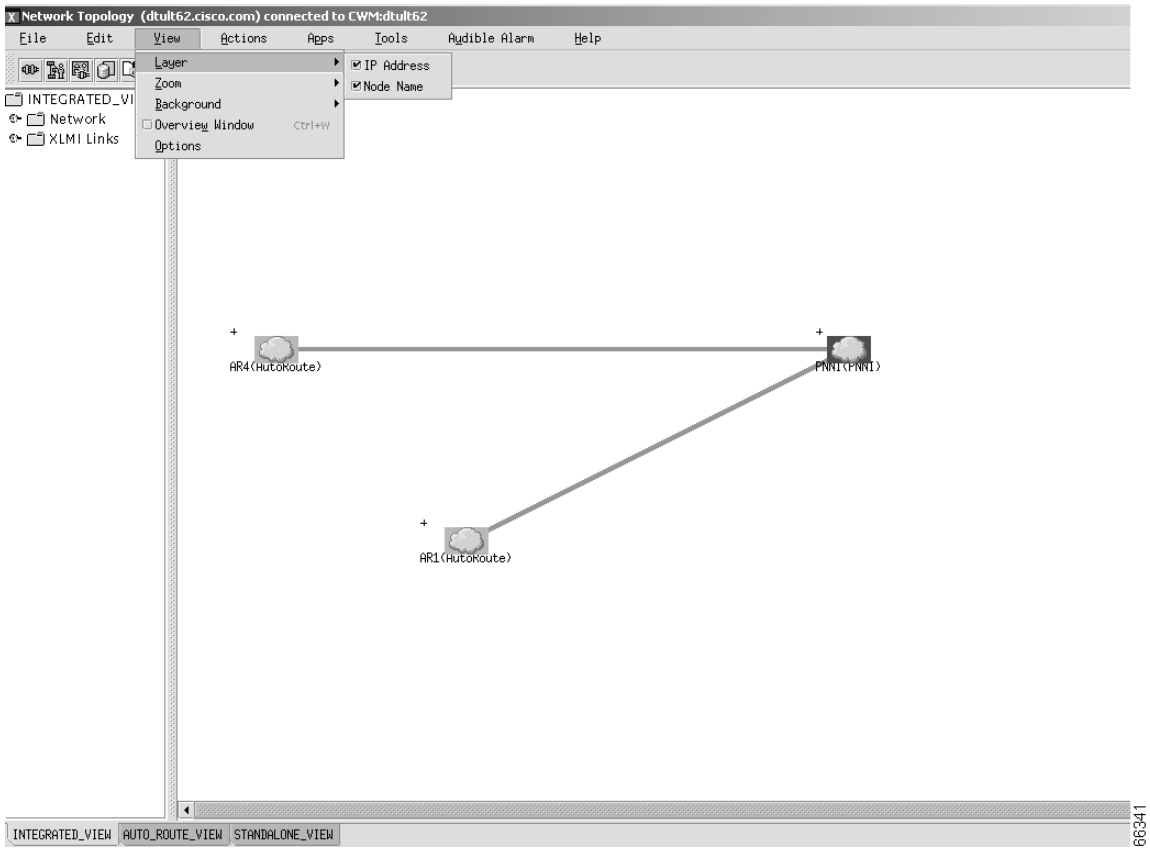
- Layer
- Zoom
- Background
- Overview Window
- Options

Note The mnemonic to open the view menu is to press the Alt and V keys simultaneously.

Layer

The **Layer** option, shown in Figure 3-4, is a submenu which allows the user to display the **IP address**, or turn off the display of the IP address, as well as displaying the **Node Name** off or on.

Figure 3-4 View Menu- Layer Submenu



Zoom

The **Zoom** option, shown in Figure 3-5, is a submenu which provides different levels of zoom functions.

Zoom (Percentage)

The **Zoom** option zooms the current submap, or window, by the percentage you choose:

- 25%
- 50%
- 100% (actual size)
- 200%
- 400%

Fit in Window

The **Fit in Window** option fits all objects in the current submap into the available space on the submap.

Mnemonic	Accelerator
None	Ctrl + F

Custom Zoom

The **Custom Zoom** option displays a dialog box allowing you to provide a specific percentage to zoom the current submap.

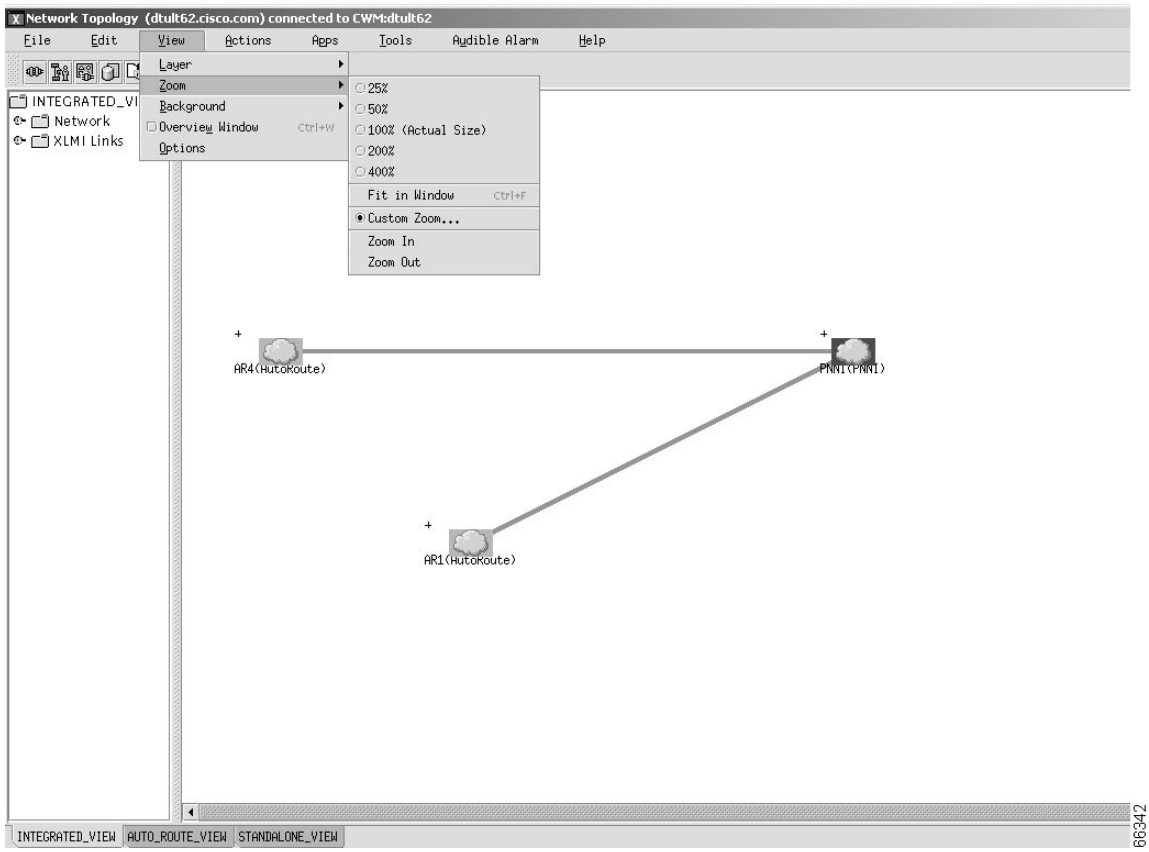
Mnemonic	Accelerator
None	Ctrl + M

Zoom In / Zoom Out

The **Zoom In/ Zoom Out** option zooms in or zooms out of the current submap image.

Zoom In Accelerator	Zoom Out Accelerator
NumPad +	NumPad -

Figure 3-5 View Menu- Zoom Submenu



Background

The **Background** option, shown in Figure 3-6, is a submenu which provides the following functions:

Set Color

The **Set Color** option sets the background color of the current submap, or clears the background color of the current submap.

Set Map

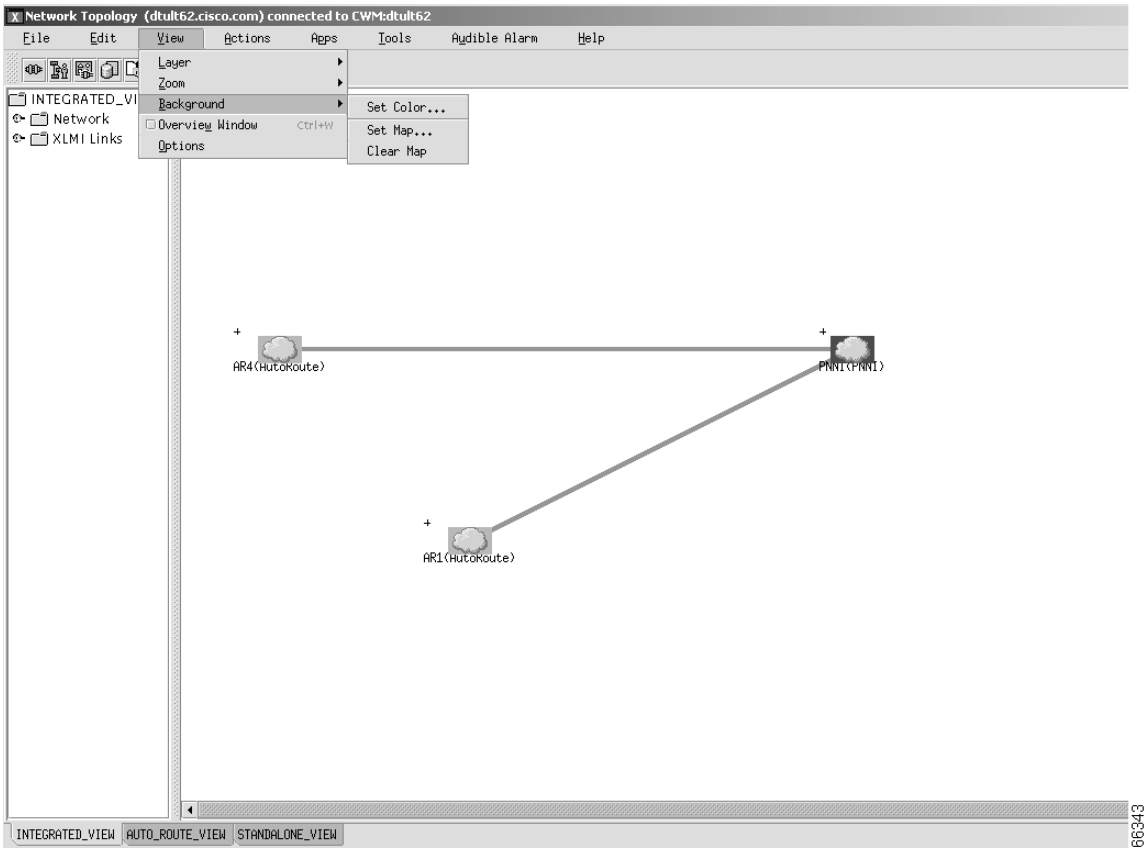
The **Set Map** option brings up a directory window that allows you to save a Topology background map by choosing from a variety of ILV images.

Note CWM currently ships with a base set of ILV images. Use these ILV images (background maps) to avoid resolution problems that can occur with images in other formats such as .gif or .jpg. Additional images may be used by copying a new image to the image directory.

Clear Map

The **Clear Map** option clears the background image in the current submap.

Figure 3-6 View Menu- Background Submenu



Overview Window

The network topology **Overview Window** option provides a complete view of the topology map.

Options

Options is a submenu which provides a window with **Navigation** and **Background Image** panels. Selecting the **Navigation** panel allows you to choose between:

- Open each submap in the same window
- Open each submap in its own window

Selecting the **Background Image** panel allows you to Display Style using the following options:

- Hide Image
- Center Image
- Tile Image
- Stretch Image

The **Background Image** panel also allows you to set magnification through the Image Scale.

Note The contents of the **Background Image** panel will be enabled if a background image has been selected.

Actions Menu

The **Actions** menu, shown in Figure 3-7, provides the following options which directly change the current view of network topology:

- Network
- Node
- Trunk
- Group

Note The mnemonic to open the action menu is to press the Alt and A keys simultaneously.

Network

The **Network** submenu option enables the display of the following views:

Display Link Status

The **Display Link Status** option displays the link status of all nodes in the current submap.

Note This option is only applicable to auto route (AR) networks.

VSI Consistency Check

The **VSI Consistency Check** option brings up a Display VSI Resource Check dialog box which lists errors and VSI trunk end partition information.

Note This option is only applicable to auto route (AR) networks.

Expand Network InView

To see an expanded view of the network, first highlight the network you would like to view by placing the curser on the network in the CWM Topology window, and then select the **Expand Network InView** option from the **Network** submenu. You will then see an expanded view of the network in the CWM Topology window.

Expand Network InSubmap

To see an expanded view of the network in a submap, first highlight the network you would like to view by placing the curser on the network in the CWM Topology window, and then select the **Expand Network InSubmap** option from the **Network** submenu. You will then see an expanded view of the network in the current submap.

Collapse Network InView

The **Collapse Network InView** option shows a collapsed view of the selected network in the CWM Topology window.

Collapse All Network

The **Collapse All Network** option shows a collapsed view of the entire network in the Topology main window.

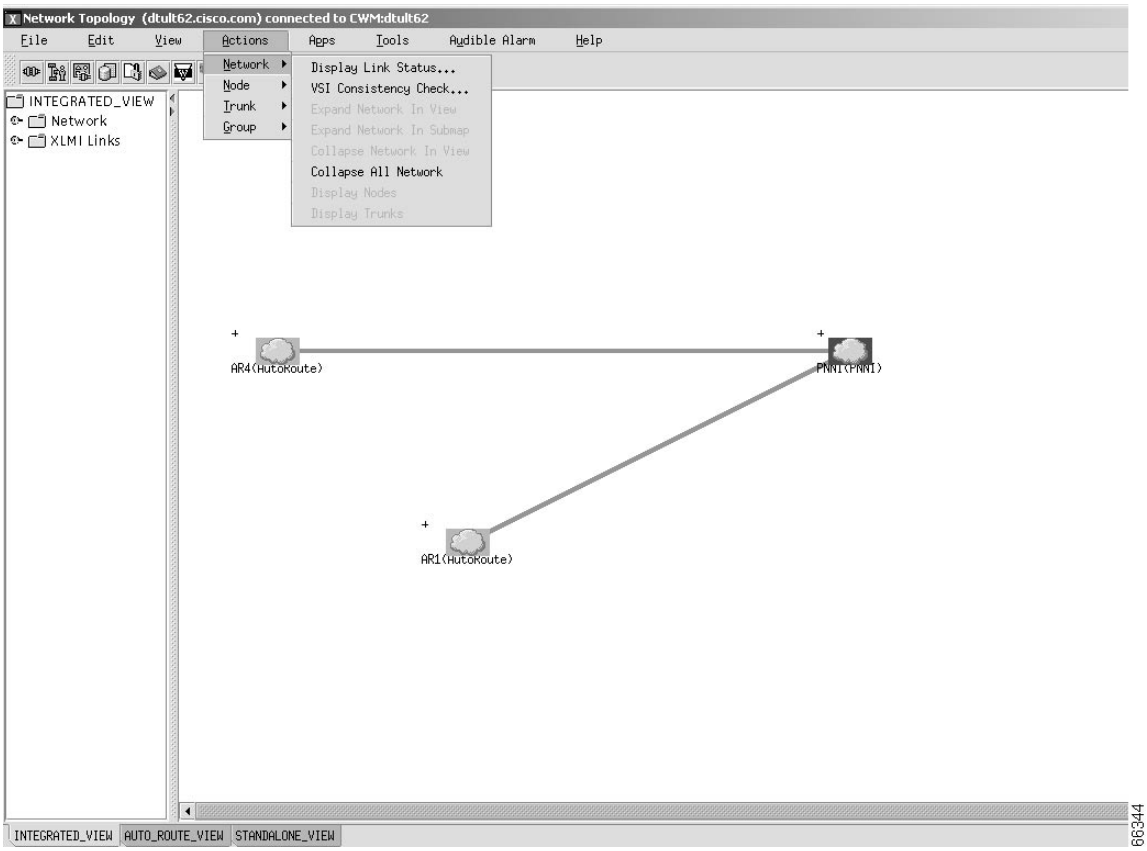
Display Nodes

The **Display Nodes** option displays all nodes.

Display Trunks

The **Display Trunks** option displays all trunks.

Figure 3-7 Actions Menu- Network Submenu



Node

The **Node** submenu option brings up a dialog box for operations specific to a selected node:

Display Shelf

The **Display Shelf** option brings up a dialog box that shows the shelves of a selected node.

Admin

The **Admin** option displays a telnet session window to connect to the selected node in the current submap.

Node Resync

The **Node Resync** option displays the Node Resync Progress dialog for the selected node in the current submap.

VSI Partition

The **VSI Partition** option displays the VSI Partition dialog box for the selected node in the current submap.

Equipment Viewer

To bring up the **Equipment Viewer** window, first select the node you would like to view from the left panel of the CWM Topology expanded tree, and then select the **Equipment Viewer** option from the **Node** submenu. The **Equipment Viewer** window appears, with a **Diagnostic** pull down menu that has **Running BERT** and **BERT Test** options for viewing diagnostics on the selected node.

Cisco View

The **CiscoView** option that is accessed from the **Actions** sub-menu (versus the **Apps** pull-down menu, as described in this chapter under the section titled, "Apps Menu"), brings up a CiscoView window that allows you to select a device *for a particular node* in which to view Telnet, CCO, Cisco Support, Preferences, About, and Help information.

XPVC Preferred Cnf

XPVC Preferred Cnf is a tool that allows users to add, modify or delete data to or from the xpvc_Pref table. If there is no entry, then no provisioning can be done. This xpvc_preferred data is used by Connection Manager and the Proxy subsystem for the provisioning of XPVCs.

The **XPVC Preferred Cnf** option brings up the XPVC Table Configurator dialog box with XPVC Preferred data displayed as **Active Entries (**contains all of the current Active entries in the xpvc_preferred table) or **Inactive Entries**.

Note When a user selects an Active entry and clicks on the **Delete** button, and an xpvc connection exists which was provisioned using this entry, it will be marked as "Inactive" and displayed as "Inactive Entries".

Nodes are listed by **Node Name**, with **Primary Lin**k and **Secondary Link** information presented in neighboring rows. The **Is Preferred** column shows whether a XPVC connection is or is not preferred.

Refresh Display, Add Entry, Modify Entry, and **Delete Entry** options are found at the bottom of the **XPVC Preferred Cnf** dialog box and are used against the xpvc_preferred table. The protocol type is automatically assigned as XPVC, provided that all user endpoints that are selected in the AR network have a xpvc_preferred table entry with the **preferred flag** set.

Note CWM will attempt XPVC provisioning on the node or its feeders, provided that all user endpoints that are selected in the AR network have an Active xpvc_preferred table entry with the preferred flag set.

Select **Node** from the **Actions** dropdown menu found on the Topology main menu bar, and then select the **XPVC Preferred Cnf** option as shown in Figure 3-8.

Figure 3-8 Actions Menu- Node Submenu

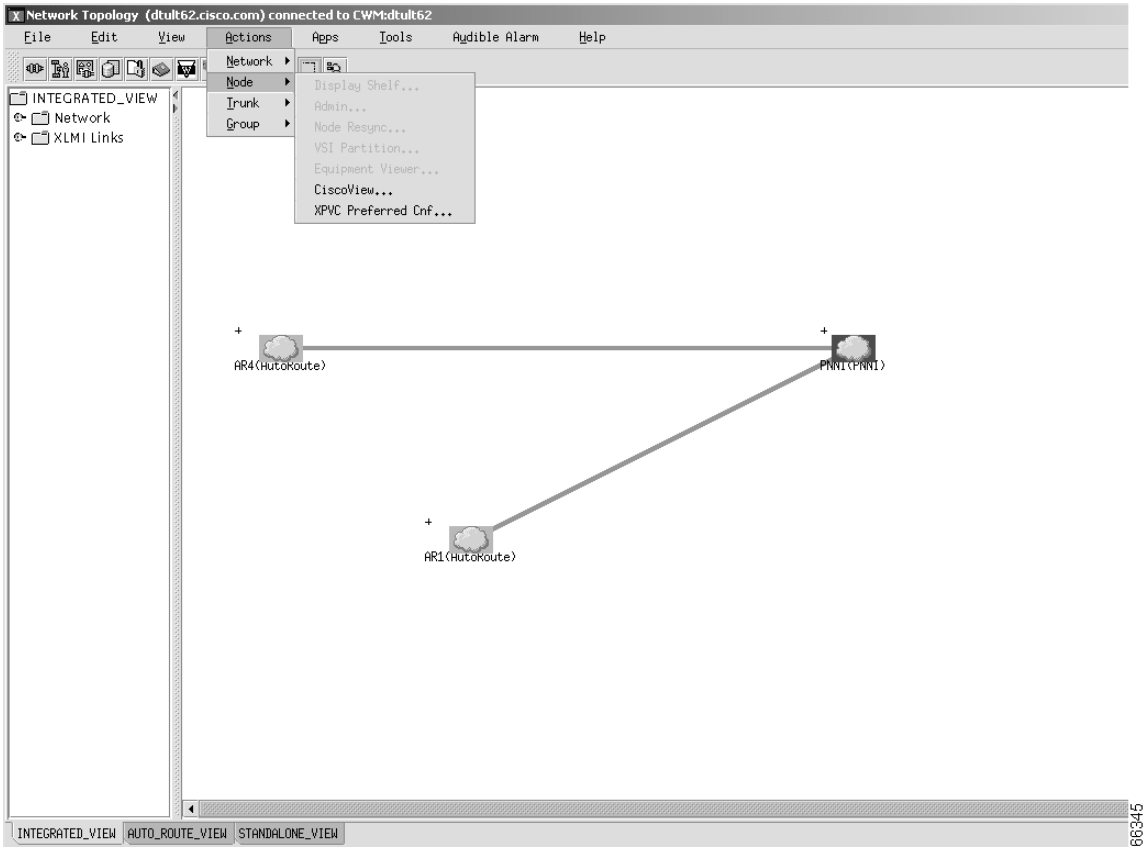


Figure 3-9 shows the XPVC preferred Table Configurator dialog box that appears after selecting the **XPVC Preferred Cnf** option found under the **Actions** pull-down menu.

Figure 3-9 XPVC Preferred Table Configurator

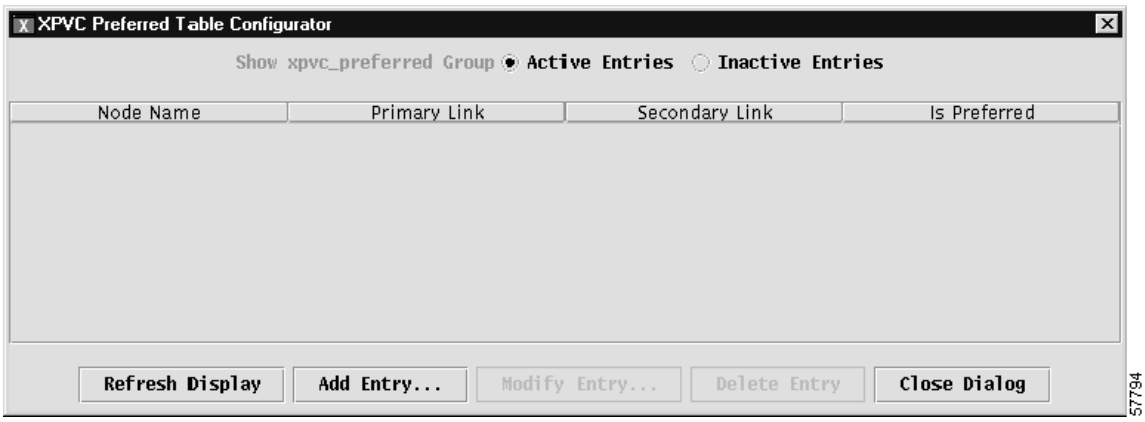


Figure 3-10 shows the XPVC Edit Entry dialog box that appears after pressing the Modify entry button from the XPVC preferred Table Configurator dialog box.

Figure 3-10 XPVC Edit Entry

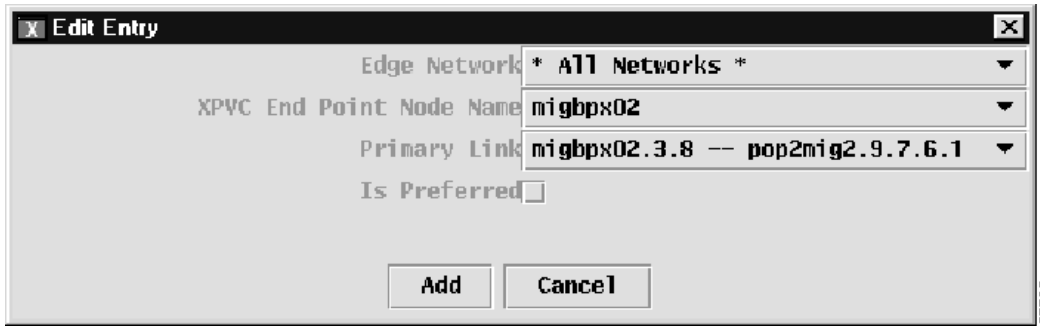
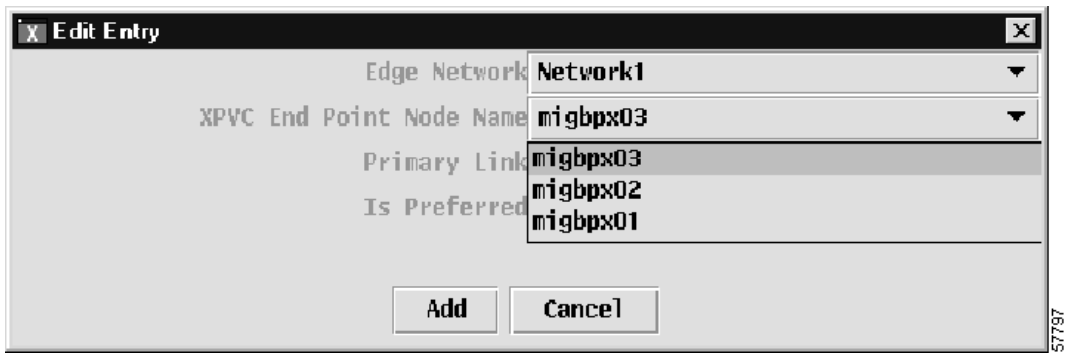


Figure 3-11 shows the XPVC Edit Entry dialog box with network nodes for Network1that appear after selecting Network1 from the Edge Network pull-down menu.

Figure 3-11 XPVC Edit Entry Network



Trunk

The **Trunk** option provides information about an individual trunk.

Display Trunk

The **Display Trunk** option displays a trunk information dialog for the selected trunk in the current submap.

Group

The **Group** option provides information about nodes and trunks.

Display Nodes

The **Display Nodes** option brings up a nodes information dialog for the selected group in the current submap.

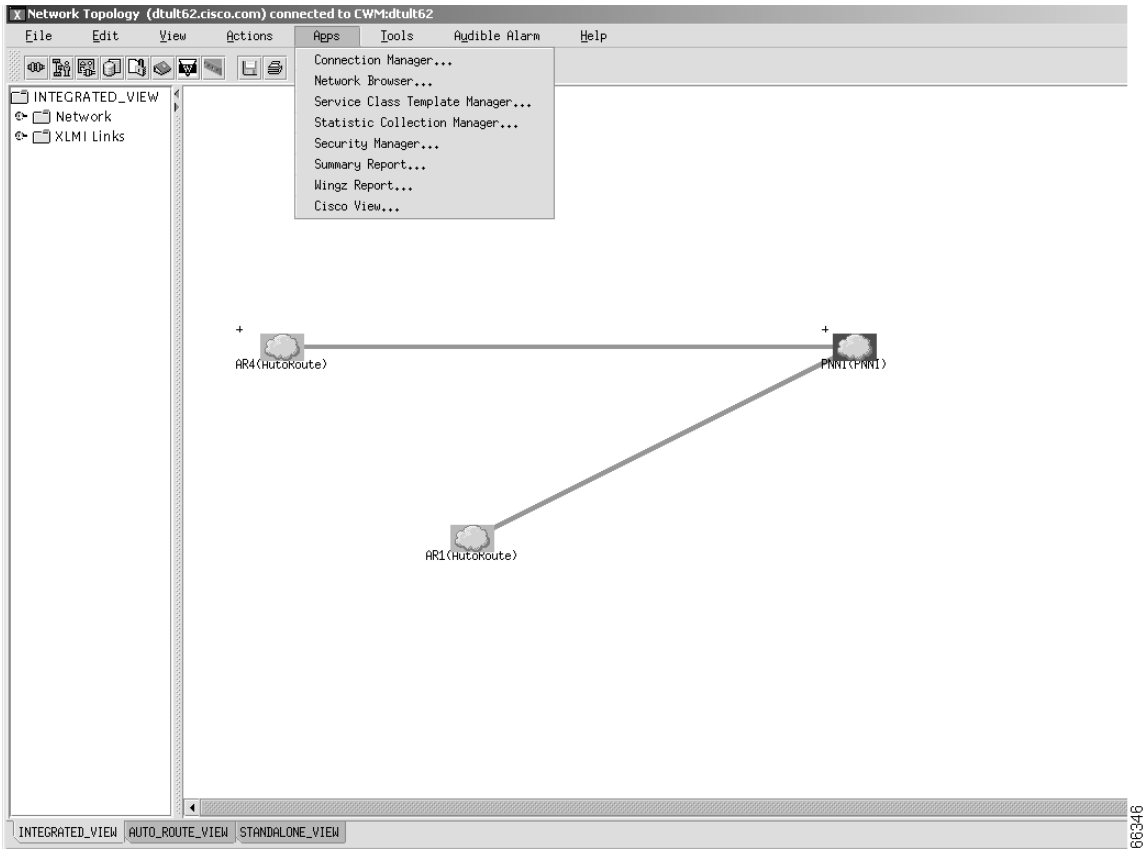
Display Trunks

The **Display Trunks** option brings up a trunks information dialog for the selected group in the current submap.

Apps Menu

The **Apps** menu, shown in Figure 3-12, provides applications that are launched from the main window of network topology, but are external to the network topology application.

Figure 3-12 Apps Menu



Connection Manager

The **Connection Manager** option launches the Connection Manager (CM) application. The CM provides the network manager the ability to add, modify, and delete end-to-end connections.

Network Browser

The **Network Browser** option launches the Network Browser application. The Network Browser displays network elements based on either a physical or logical relationship among the various network elements.

Service Class Template Manager

The **Service Class Template Manager** option launches the Service Class Template Manager (SCT) application. The SCT allows for creating SCT files which can be loaded to nodes, and associated with interfaces on cards within these nodes.

Statistics Collection Manager

The **Statistic Collection Manager** option launches the Statistic Collection Manager (SCM) application. The SCM provides a forms-based interface to establish and modify statistic collection policies for the network.

Security Manager

The **Security Manager** option launches the Security Manager application. The Security Manager provides controlled access to multiple users of CWM based on the unique user ID and password.

Summary Report

The **Summary Report** option launches the Summary Report application. CWM provides node utilization reports not based on Wingz through the Summary Report application.

Wingz Report

The **Wingz Report** option launches the Wingz Report application. CWM Statistics Reports are generated through a graphical reporting package based on the Informix Wingz Report application.

Cisco View

The **CiscoView** option brings up a CiscoView window that allows you to select a device in which to view Telnet, CCO, Cisco Support, Preferences, About, and Help information.

WAN CiscoView is a JAVA-based device management software GUI application that allows you to:

- Display a graphical representation of the network device
- Display configuration and performance information
- Perform minor configuration tasks
- Perform minor troubleshooting tasks

WAN CiscoView supports card, line, and port configuration on the MGX 8220, 8230, 8250, Release 1 and 2 of the MGX 8850, IGX 8400 series, BPX 8600 series, and BPX SES PNNI Controller.

Please see your CiscoView documentation for more details about this feature.

Tools Menu

The **Tools** menu provides operations or applications that are launched from the main window of the Network Topology, but are external to the Network Topology application.

Config Save and Restore

The **Config Save and Restore** option launches an application with In-Progress, Config Save, and Config Restore tabbed windows which allow you to view and change criteria for the selected node in the current submap.

SW/FW Images

The **SW/FW** (software/firmware) **Images** option launches the Image Download application for the selected node in the current submap.

Audible Alarm Menu

Configuration

Displays an Audible Alarm Configuration window with an editable Beep Time Interval in milliseconds, and Enable and Continuous option settings.

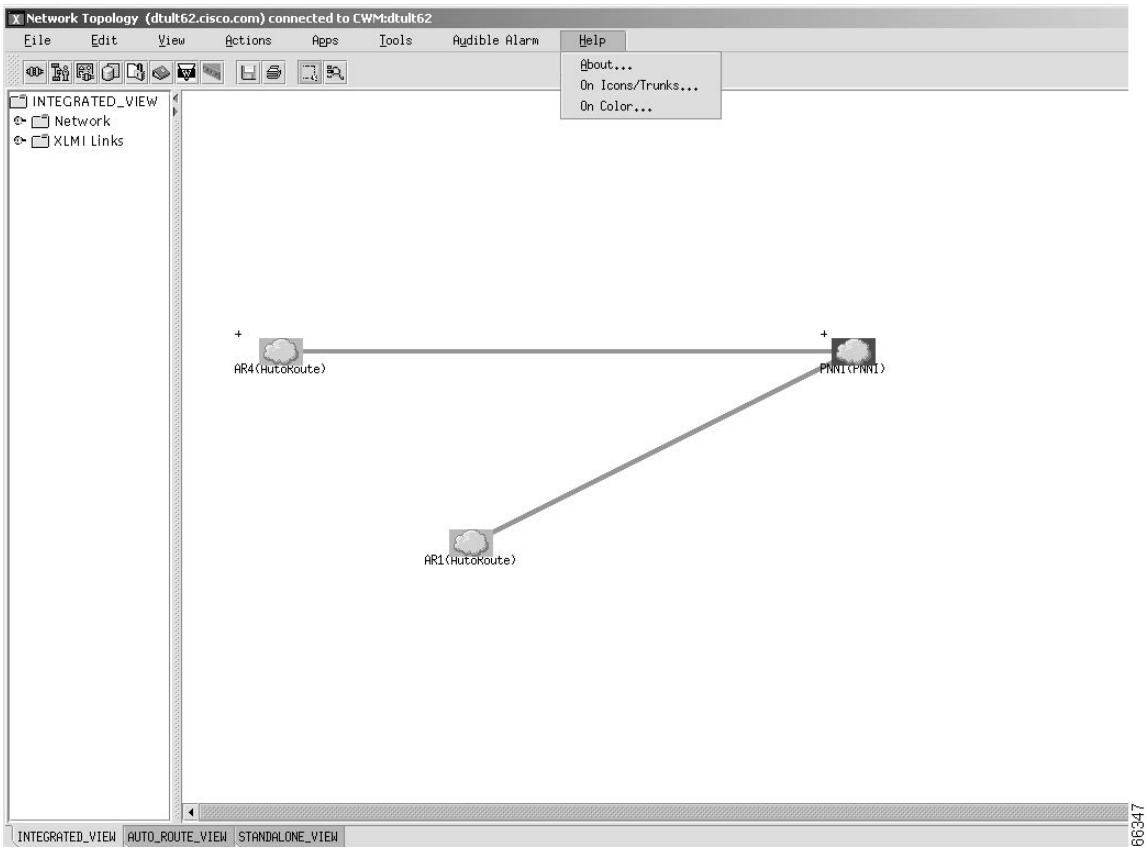
Acknowledge

Acknowledges Audible Alarm setting.

Help Menu

The **Help** menu, as shown in Figure 3-13, provides submenus with **About** and **Help** information which are described below.

Figure 3-13 Help Menu



About

Information about this version of the CWM Network Topology GUI.

Help On Icons/Trunks

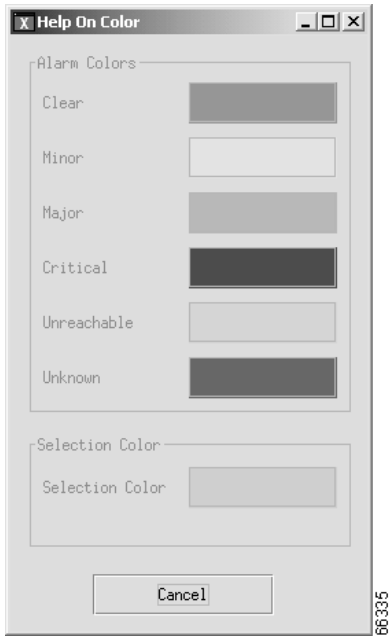
Information about how to interpret the icons displayed in the topology graph window. These Help windows are shown in Figure 3-14 and Figure 3-15.

Figure 3-14 Help On Icons/Trunks

Help On Color

Information about how to interpret the color of the icons displayed in the topology graph window.

Figure 3-15 Help On Color



Right Click Options

Submap and submenus provide an easy way to change the view of the Network Topology.There are two ways to access submaps and submenus on the Network Topology. Either right click on a node in the topology window to display the following pull down menu options:

The **Navigation** submenu provides **Inplace Submap, New Submap,** and **Overlay Submap,**

The **Network** submenu provides **Display Link Status, VSI Consistency Check, Expand Network in View, Expand Network in Submap, Collapse Network in View, Collapse all Network, Display Nodes,** and **Display Trunks** options. These options are also found under the **Actions** menu, described earlier in this chapter.

The **Group** submenu provides **Add Node, Delete Node, Delete, Display Nodes, and Display Trunks** options. These options are also found under the **Edit** menu, described earlier in this chapter.

The **Node** submenu provides **Display Shelf, Admin**, **Node Resync**, **VSI Partition, Equipment Viewer, CiscoView,** and **XPVC Preferred Cnf** options. These options are also found under the **Actions** menu, described earlier in this chapter.

To access additional submaps and submenus, right click in the Topology window outside of a node area. The following pull down menu options are displayed:

The **Network** submenu provides **Display Link Status, VSI Consistency Check, Expand Network in View, Expand Network in Submap, Collapse Network in View, Collapse all Network, Display Nodes,** and **Display Trunks** options. These options are also found under the **Actions** menu, described earlier in this chapter.

The **Navigation** submenu provides **Show Parent Map** and **Show Root Map** submap options.

The **Background** submenu provides **Set Color, Set Map and Clear Map** options. These can also be found under the **View** menu described earlier in this chapter. In addition to these options, the **Background** menu provides **Color, Monochrome, Less Contrast and More Contrast** options.

Navigation Submaps

Inplace Submap

The **Inplace Submap** option creates an encased submap of the selected node.

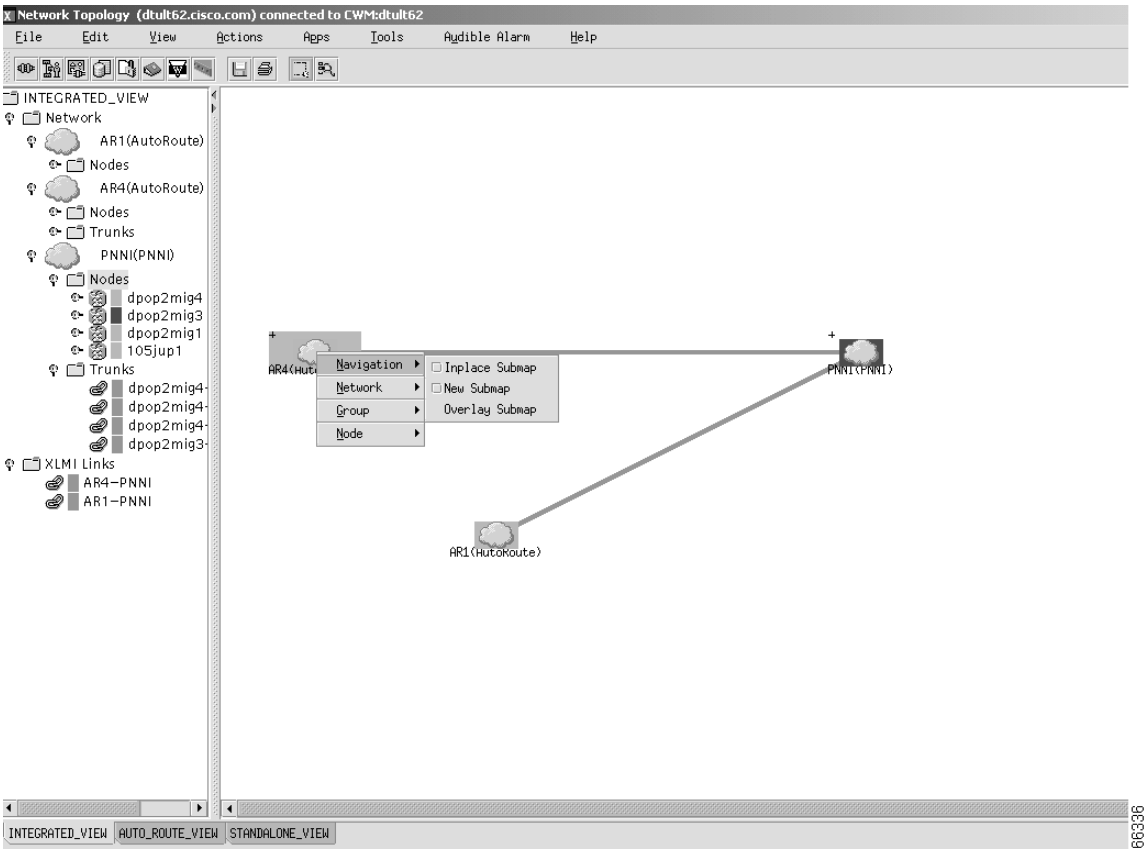
New Submap

The **New Submap** option creates a new submap within the current Topology.

Overlay Submap

The **Overlay Submap** option overlays the nodes on the current Topology.

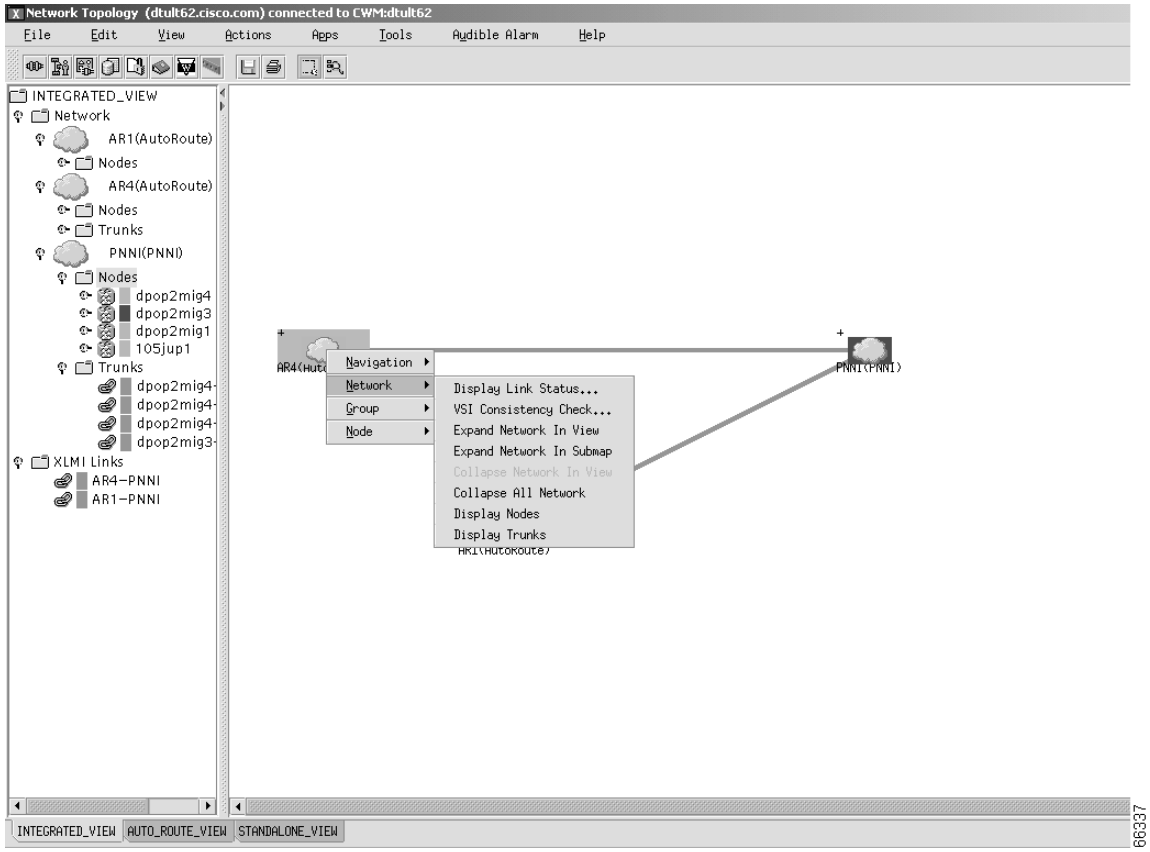
Figure 3-16 Navigation Submaps



Network Submenu

The **Network** submenu, as shown in Figure 3-17, provides **Display Link Status, VSI Consistency Check, Expand Network in View, Expand Network in Submap, Collapse Network in View, Collapse all Network, Display Nodes,** and **Display Trunks** options. These options are also found under the **Actions** menu, described earlier in this chapter.

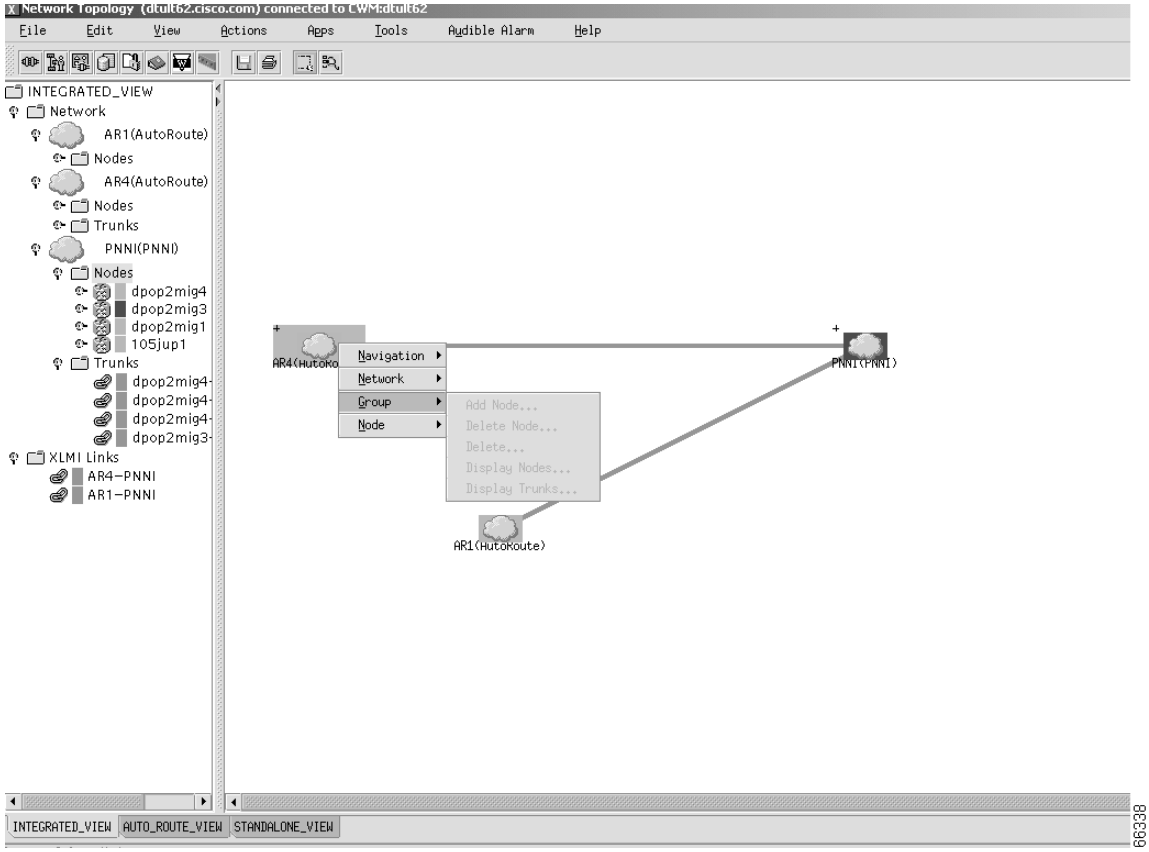
Figure 3-17 Network Submenu



Group Submenu

The **Group** submenu, as shown in Figure 3-18, provides **Add Node, Delete Node, Delete, Display Nodes, and Display Trunks** options. These options are also found under the **Edit** menu, described earlier in this chapter.

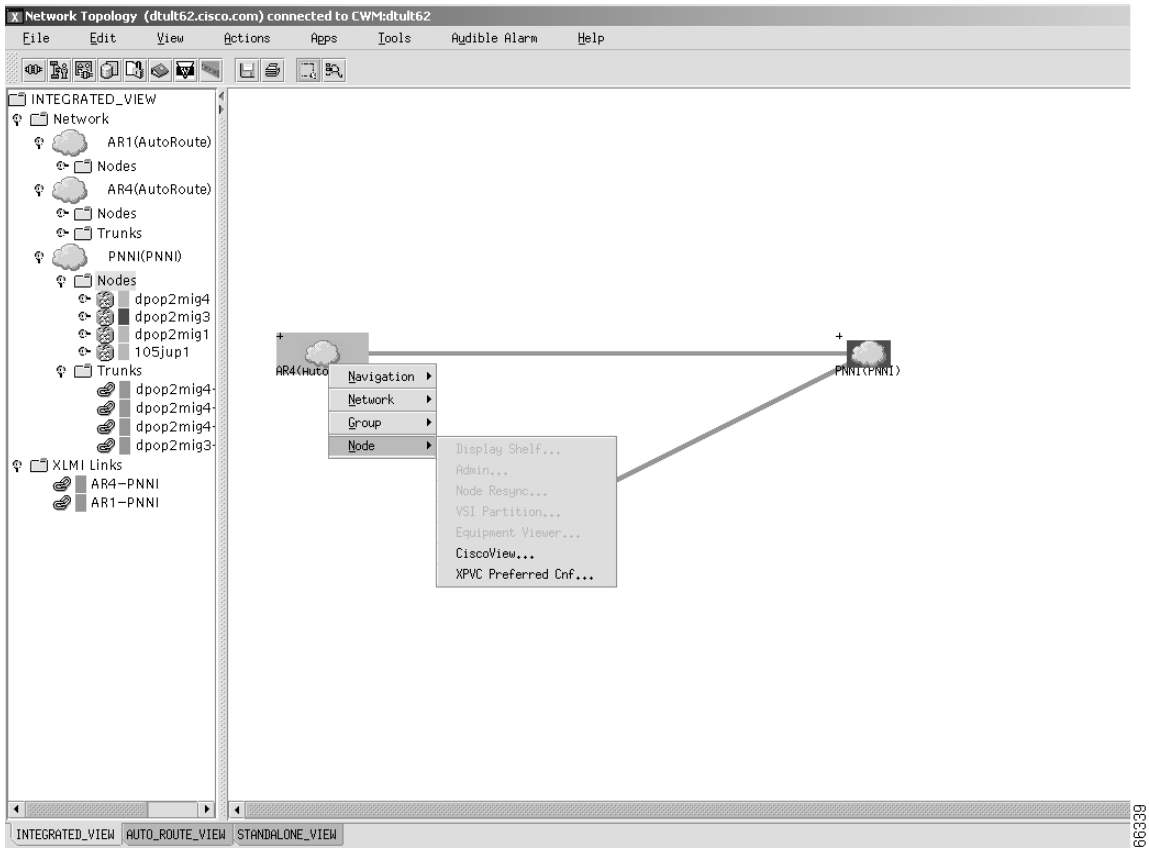
Figure 3-18 Group Submenu



Node Submenu

The **Node** submenu, as shown in Figure 3-19, provides **Display Shelf, Admin**, **Node Resync**, **VSI Partition, Equipment Viewer, CiscoView,** and **XPVC Preferred Cnf** options. These options are also found under the **Actions** menu, described earlier in this chapter.

Figure 3-19 Node Submenu



Save Button

The save button provides the same function as the Save option of the File menu.

Select Button

The select button enables you to select an object in the current submap, perhaps to drag to a different location on the map or upon which to perform another action.

Zoom Button

This zoom button zooms out the selected objects during a drag operation.

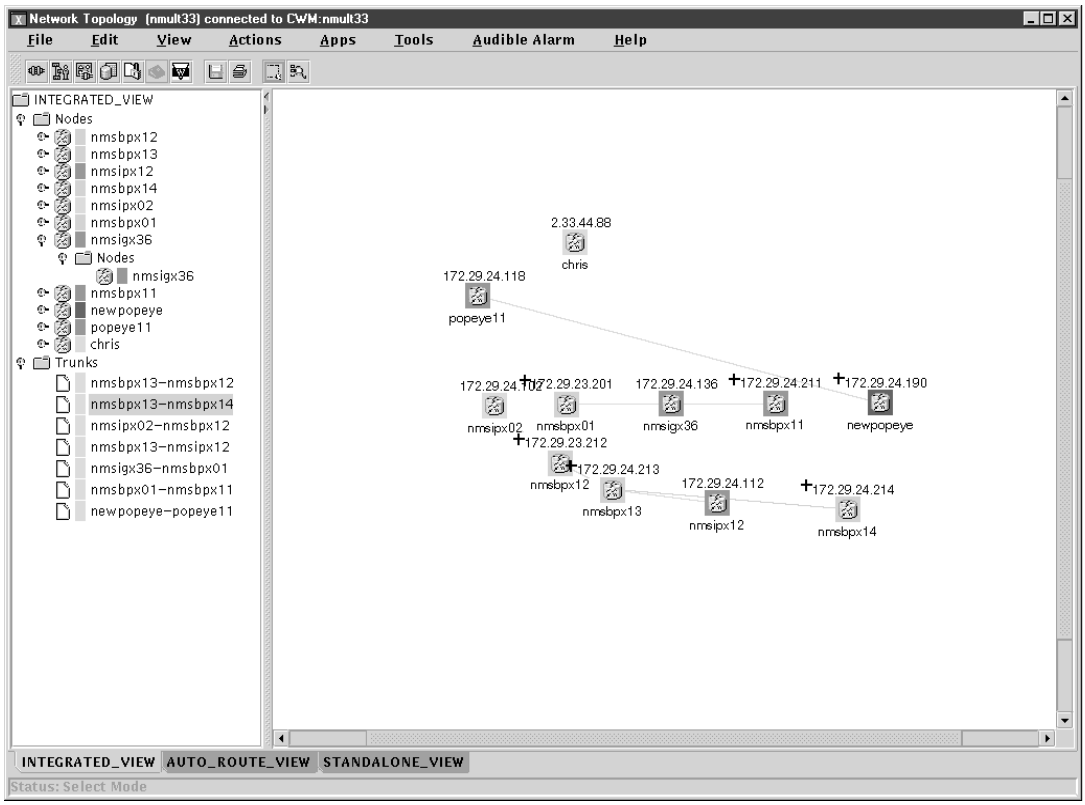
Print Button

The print button provides the same function as the Print option of the File menu.

Using the Hierarchy Tree

The network topology hierarchy tree provides a list view of all available topology information.

Figure 3-20 Expanded View of Network Topology Hierarchy



Interaction with the Hierarchy Tree

When first displayed, the network topology hierarchy tree displays only the top-level objects. By clicking on the object, you can expand its view to display any child objects it contains.

Network Alarm Colors

CWM uses color to display alarm situations detected by the Network Topology:

- Normal (green)
- Minor (yellow)
- Major (orange)
- Critical (red)
- Unreachable (gray)
- Unknown (blue)

Connection Manager

This chapter describes the CWM Connection Manager (CM) desktop application. You use the Connection Manager to create and maintain end-to-end connections, Permanent Virtual Circuits (PVCs), or Soft Permanent Virtual Circuits (SPVCs). A connection consists of a source (*localEnd*), a destination (*remoteEnd*) and a set of connection parameters required for the routing.

Connection Manager Overview

You can have up to four Connection Manager windows per CWM desktop session running on your workstation at any one time (though only one can be started from the CWM Desktop; the others must be started from a Connection Manager window's **File** menu).

The Security Management feature, in which each CWM user has their own access profile, is used to determine whether you have the rights to use each option in the CWM Connection Manager. The security mapping for CWM Connection Manager is:

- If you have Read Permission you can list connections.
- If you have Create Permission, you can add new connections and perform diagnostics. In addition, you have Read Permission privileges.
- If you have Modify Permission, you can modify connections. In addition, you have Read Permission privileges.
- If you have Delete Permission, you can delete connections. In addition, you have Read Permission privileges.
- If you have All permissions, you can do all of the above.

Supported Connection Types

Release 10 of Cisco WAN Manager supports the following connections:

- Asynchronous Transfer Mode (ATM)
- ATM Router Processor Module
- VISM
- Frame Relay (FR)
  - Frame Relay
  - Frame user network interface (FUNI)

  - Frame forwarding
- Circuit Emulation (CE)
- Voice and Data service modules

Supported Card Types

Table 4-1 lists the types of cards supported in CWM and the different cards in each card type.

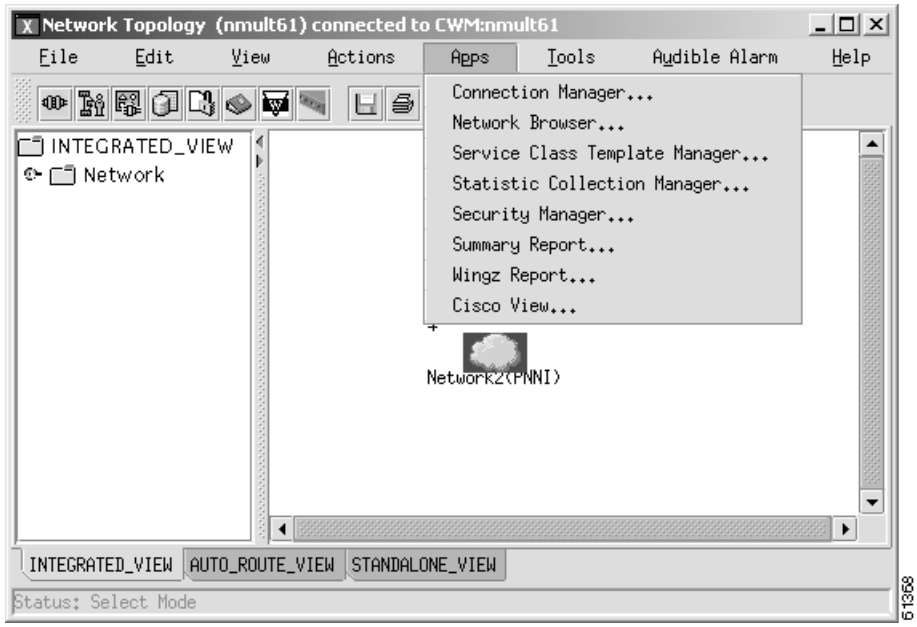
Table 4-1 Supported Card Types in CWM

Card Type	Cards Supported
ATM	AUSM (4T1, 4E1, 8T1, 8E1), AUSMB (8T1, 8E1), PXM (T3, E3, OC3, OC12), ASI (T3, E3, OC3), ASI-155, BXM (OC3, OC12,T3, E3), UXM, BXME (OC3, OC12)
AXSM, AXSMB	AXSM-OC3, AXSM-OC12, AXSM-OC48, AXSM-T3E3
CE	CESM (4T1, 4E1, 8T1, 8E1, T3, E3)
Data Service Modules	CVM, UVM, HDM, LDM, SDP, LDP
FR	FRSM (4T1, 4E1, 8T1, 8E1, HS1b.V35), FRM, UFM, FRP
FRSM-VHS	FRSM (2CT3, 2E3, 2T3, HS2), FRSM (HS2B)
RPMB, RPM-PR	RPM-PR
Voice Service Modules	CVM, UVM, CDP, VISM

Starting Connection Manager

To start Connection Manager, first start the CWM Desktop from the CWM **Main Menu**, as described in Chapter 2, “Starting and Stopping Cisco WAN Manager.” Then, to bring up the Connection Manager application, either click on the CWM desktop window’s **Connection Manager** icon, or select **Connection Manager** from the **Apps** pulldown menu. Both options are shown in Figure 4-1.

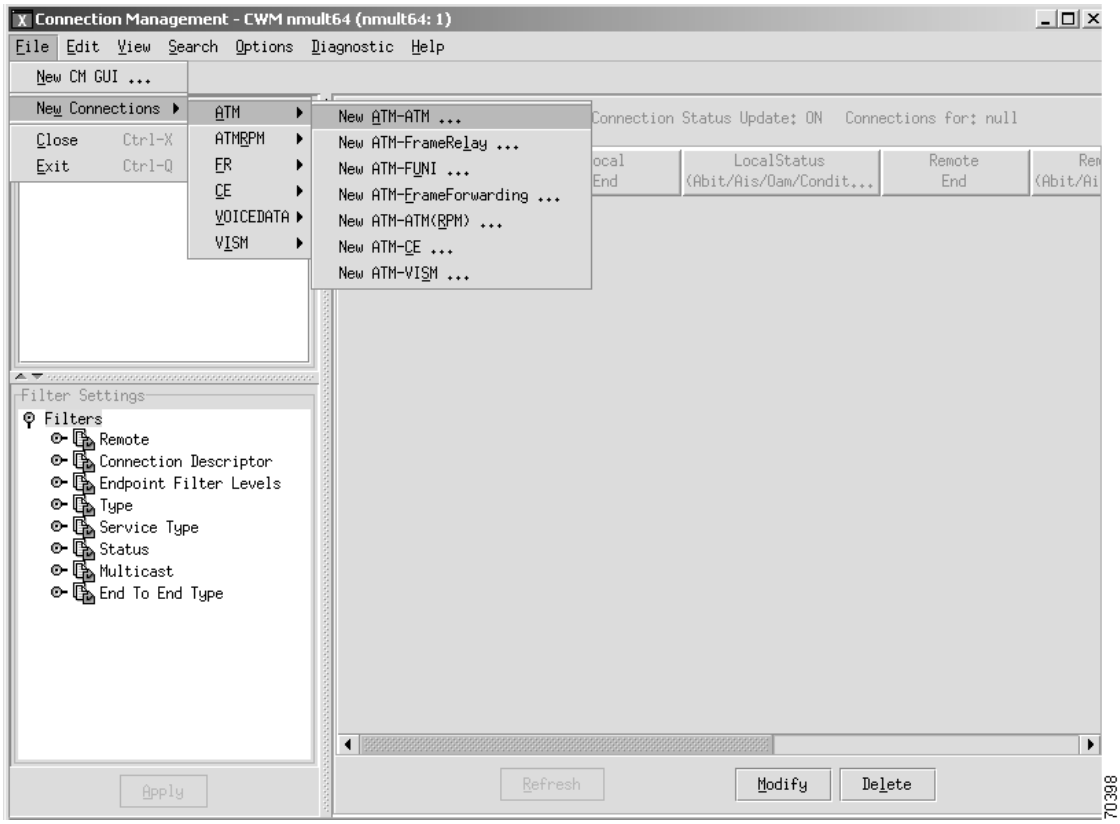
Figure 4-1 CWM Desktop Window



The CWM Connection Manager window is displayed in Figure 4-2. Use this window to browse the list of established connections, as well as to invoke the other CWM Connection Manager features.

A **New ATM-ATM** connection option is shown in Figure 4-2. Use the **File** dropdown menu to select **New Connections** and display a list of available connection options.

Figure 4-2 CWM Connection Manager Window



Platform, Card, and Connection Types

Platform Types

The following platforms are supported for provisioning XPVC user endpoints:

- BPX 8600
- AXIS 8220
- MGX 8230, MGX 8250 and MGX 8850-R1
- MGX 8850-R2

The following platforms are supported as via nodes, but are not supported for XPVC user endpoints creation:

- IGX 8400

Card Types

The following cards are supported for XPVC user endpoints:

- BXM and BXM-E
- ASI

- PXM1
- AXSM
- AUSM
- FRSM
- RPM
- RPM-PR (can be on both MGX1 & MGX2)

The following cards are not supported as user endpoints:

- CESM
- VISM
- Cards from IGX

XPVC Connection Types

Connection Types for AR-PNNI-AR XPVC

The following 3 segment XPVCs are allowed:

ATM-ATM

- AUSM-AUSM, AUSM-PXM1, AUSM-BXM, and AUSM - RPM/RPM-PR
- PXM1-PXM1, PXM1-BXM, and PXM1 - RPM/RPM-PR
- BXM-BXM, and BXM - RPM/RPM-PR
- RPM/RPM-PR- RPM/RPM-PR

ATM-FR

- AUSM-FRSM
- PXM1-FRSM
- BXM-FRSM
- RPM/RPM-PR - FRSM

FR-FR

- FRSM-FRSM

Connection Types for AR-PNNI

ATM-ATM

- AUSM-AXSM
- PXM1-AXSM
- BXM-AXSM
- RPM-AXSM
- AUSM - RPM-PR

- BXM - RPM-PR
- PXM1 - RPM-PR
- RPM/RPM-PR - RPM-PR

FR-ATM

- FRSM-AXSM
- FRSM - RPM-PR

Connection Types for AR-Hybrid

ATM-ATM

- AUSM-AUSM, AUSM-PXM1, and AUSM-RPM/RPM-PR
- PXM1-AUSM, PXM1-PXM1, and PXM1-RPM/RPM-PR
- BXM-AUSM, BXM-PXM1, and BXM-RPM/RPM-PR
- RPM/RPM-PR -AUSM, RPM-PXM1, and RPM/RPM-PR - RPM/RPM-PR

ATM-FR

- AUSM-FRSM
- PXM1-FRSM
- BXM-FRSM
- RPM/RPM-PR - FRSM

FR-ATM

- FRSM-AUSM
- FRSM-PXM1
- FRSM - RPM/RPM-PR

Connection Manager Main Window

The Connection Manager main window includes the following components:

- Menu bar—Provides available menu options for the connection manager application.
- Tool bar—Contains the most frequently used actions in icon format.
- Button panel—Contains navigational buttons.
- Start node tree—Displays the full path of the currently selected node.
- Filter settings tree—Displays the filter categories and values currently selected.
- List of connections—Lists a subset of connections managed by CWM based on the selected start node and filter values.
- Status bar—Displays any errors or informational messages as you attempt to perform various actions.

Menu Bar

The Connection Manager menu bar provides actions that you can select by pulling down the menu and clicking on the desired action. The following menus and submenus are available:

- **File**
  - **New CM GUI**—Opens a new instance of Connection Manager application. You can have up to four instances of the Connection Manager running at any one time on a workstation.
  - **New Connections**—Displays a list of available connection types from which to select when adding a new connection.
  - **Close**—When you are running multiple instances of the Connection Manager, selecting this action closes the current Connection Manager main window. If you are running only one instance, selecting this action returns you to the CWM main menu.
  - **Exit**—Exits the Connection Manager application.
- **Edit**
  - **Filters**—Displays the Filter Settings Dialog Box.
  - **Delete Template**—Displays the Delete Template Dialog Box that lists the templates that can be deleted.
- **View**
  - XPVC Segments—Displays the XPVC Connection and Segments window.
  - **Alarm Console**—Displays the Alarm Console log.
  - **MultiCast Group**—Displays members of the MultiCast Group.
- **Diagnostic**
  - **Test Connection**—Tests the integrity of a connection between a card and the remote end within the WAN switching network by sending a single collection of supervisory cells to the remote end. The terminal displays only a pass or fail message.
  - **Test Delay**—Externally tests the integrity of a connection by sending a single collection of supervisory cells to the remote end of the network and back. The terminal displays a passor fail message and the round trip time in milliseconds.
  - Search option
  - **Connection Trace**—Displays connection trace information.
  - **Detailed Status**—Displays detailed status and configuration information for a specified group.
  - **Reroute**—Displays the reroute timer settings.
  - **Connection Up**—Allows you to up a connection.
  - **Connection Down**—Allows you to down a connection.

Note When trying to start Bert through the BERT GUI, the GUI allows you to change parameters that are not applicable to AXSM-E T1 lines. From the GUI, the only configurable parameters are Inverse pattern at TX, Inverse pattern at Rx, and Insert constant-rate error for AXSM-E T-1 lines.The other parameters should not be modified.

- **Help**
  - **Help**—Displays Connection Manager version information.

Tool Bar

The Connection Manager tool bar contains icon buttons that access frequently used actions. The following icons are available:

- Delete Template
- Edit Filter
- Help

Button Panel

The Connection Manager button panel contains the following navigational buttons:

- Apply—Allows you to apply selected filters to the list of connections.
- Refresh—Allows you to refresh the list of connections from the Connection Manager server, but not apply any new filters to the connections.
- Modify—Allows you to modify a connection's parameters.
- Delete—Allows you to delete connections.

Start Node Tree

The Connection Manager Start Node Tree shows the network equipment that is being managed by CWM. You can select any node from the hierarchy to be the current start node. The label on the top of this pane shows the current selected node.

Filter Settings Tree

The Connection Manager Filter Settings Tree displays the filter categories and values currently selected. Click the **Apply** button to review the selected connection types.

List of Connections

The Connection Manager List of Connections lists a subset of connections managed by CWM based on the selected start node and filter values.

Status Bar

The Connection Manager Status Bar displays any errors or informational messages as you attempt to perform various actions.

Alarms and Events

After selecting a node from the Start Node Tree, or any slot, line, or port under a node in the tree, and then selecting the **Apply** button, the Connection Manager will update alarms and events on selected connections under the following circumstances:

- The Connection Dialogue window appears with the number of connections matching the filtering criteria. If you select **Get All** or **Get <n>** connections, and then select the **OK** button, the connections will be listed in the List of Connections window. Any event or alarm for these connections will now be dynamically refreshed.
- The Connection Dialogue window appears with the number of connections as "0". In this case, the user should select **Get All** and then select the **OK** button. Any event or alarm for all newly created connections, with at least one endpoint on the selected node, will now be dynamically refreshed.

Note If the newly added connections do not have at least one endpoint on the selected node, then no alarms or events will be refreshed for those connections.

Configuring Connections

To configure a connection, complete the following steps:

Step 1 Log in to the CWM workstation as a user with access privileges that allow you to create connections using Connection Manager.

Step 2 If necessary, start CWM and launch the desktop.

Step 3 Select Connection Manager.

Step 4 Select a Connection Mode

Step 5 Select a connection type from the list of connections.

Further configuration of your connection depends on the connection type. The following endpoints/cards are supported in Release 10 of the CWM Connection Manager:

- MGX 8220
  - FRSM-4, FRSM-8, and FRSM-HS1 (Frame Relay)
  - FRSM-VHS - 2CT3, 2E3, 2T3, and HS2 (Frame Relay)
  - AUSM-4 and AUSM-8 (ATM)
  - CESM-4 (T1, E1) and CESM-8 (T1, E1) (Circuit Emulation)
  - CESM-1 T3/E3 (Circuit Emulation)
  - HS2B card
- MGX 8850 Release 1
  - FRSM-2CT3
  - FRSM- 2T3/E3
  - FRSM-HS2
  - FRSM-8 T1/E1
  - CESM-1 T3/E3
  - CESM-8 (Circuit Emulation)
  - PXM-UNI
  - VISM (T1, E1)

  - HS2B card
- MGX 8850 Release 2
  - PXM-45
  - RPM-PR
  - AXSM
  - AXSMB
- **BPX 8600**
  - BXM and ASI (ATM)
  - BME
  - BXME
- BPX with SES feeder node
  - BXM
- IGX 8400
  - UXM (ATM)
  - FRM, UFM, and UFM-U (Frame Relay)
  - CVM and UVM (Voice)
  - CVM, HDM and LDM (Data)
  - SDP and LDP (Data)

Connection Modes

The CWM Connection Manager supports the following connection mode:

- **Normal**—normal/regular PVCs

Configuration Management

Operations supported in **Normal** mode:

- browse connection list
- browse Root to Leaf connectivity for multicast
- add a new connection
- modify a connection
- delete a connection
- verify *TestContinuity*
- verify *TestDelay*

Connection types supported in **Normal** mode:

- Frame Relay to Frame Relay
- ATM to ATM
- ATM to Frame Relay

- CE to CE (Circuit Emulation)
- Voice to Voice
- Data to Data
- ATM to CE
- RPM to RPM
- RPM to ATM
- RPM to FR
- VISM to ATM
- VISM to VISM

Note Verification of Test Continuity and Test Delay is not supported for connections that involve RPM endpoints.

Connection Manager Window Menus

Menu options in the Connection Manager window are:

File - New Connection Manager

Select this option to start another instance of the Connection Manager program. You can have up to four instances of the Connection Manager running at any one time on a workstation. Only one can be started from the CWM Desktop; the others must be started from the **File** menu of one of the running programs.

File - Exit

Select this option to exit the Connection Manager. This option works only on the window in which the option is selected. When you have started other Connection Managers, they continue to run.

View - View Multicast Connections

Select this option to browse multicast connections. This menu item remains disabled when the selected connection is not the correct type for this option.

Configure - New FR-FR Connection

Select this option to create a new FR-FR connection.

Configure - New ATM-ATM Connection

Select this option to display a submenu, which allows you to view a new ATM-ATM Connection window with fields appropriate to one of the following service types:

- CBR.1
- VBR.1 (NRT, VBR.1 RT)
- VBR.2 (NRT, VBR.2 RT)
- VBR.3 (NRT, VBR.3 RT)

- ABR.FS
- ABR.1
- UBR.1
- UBR.2
- ATFST
- ATFXFST
- ATFTFST

Configure - New ATM-RPMB Connection

Select this option to display a submenu, which allows you to view a new ATM-RPMB Connection window with fields appropriate to one of the following service types:

- VBR.3
- ABR
- UBR.1
- UBR.2

Configure - New ATM-FR Connection

Select this option to display a submenu, which allows you to view a new ATM-FR Connection window with fields appropriate to one of the following service types:

- CBR.1
- VBR.1
- VBR.2
- VBR.3
- UBR.1
- UBR.2
- ABRFS
- ABR.1

Configure - New CE-CE Connection

Select this option to create a new CE-CE connection.

Configure - New Voice Connection

Select this option to create a new Voice connection.

Configure - New Data Connection

Select this option to create a new Data connection.

Configure - New ATM-CE Connection

Select this option to create a new ATM-CE connection.

Configure - New ATM-VISM Connection

Select this option to create a new ATM-VISM connection.

Configure - New VISM-VISM

Select this option to create a new VISM-VISM connection.

Supported Connection Service Types and Protocols

Release 10 of Cisco WAN Manager supports the following connections:

- Asynchronous Transfer Mode (ATM)
- ATM Router Processor Module (ATM-RPM)
  - Frame Relay (FR)
  - ATM
  - RPM
- Frame Relay
  - FR
  - Frame User Network Interface (FUNI)
  - Frame Forwarding
- Circuit Emulation (CE)
- Voice and Data service modules
- VISM

When adding a new connection from the Connection Manager application, you are asked to specify the service type and protocol.

The following tables list the service type and protocol selections available for each connection type.

Table 4-2 ATM Connection and Protocol Types

Connection Type	Service Types	Protocols
ATM-ATM	cbr1 vbr1_nrt vbr2_nrt vbr3_nrt vbr1_rt vbr2_rt vbr3_rt abrfs abr1 ubr1 ubr2 ATFXFST ATFTFST	PVC SPVC Hybrid
ATM-Frame Relay	cbr1 vbr2_nrt vbr3_nrt vbr2_rt vbr3_rt abrfs ubr1 ubr2 abr1	PVC Hybrid
ATM-FUNI	cbr1 vbr2_nrt vbr3_nrt vbr2_rt vbr3_rt abrfs ubr1 ubr2 abr1	PVC Hybrid
ATM-Frame Forwarding	cbr1 vbr2_nrt vbr3_nrt vbr2_rt vbr3_rt abrfs ubr1 ubr2 abr1	PVC Hybrid
ATM-ATM (RPM)	vbr3_nrt abr1 ubr1	PVC Hybrid

Table 4-2 ATM Connection and Protocol Types (continued)

Connection Type	Service Types	Protocols
ATM-CE	cbr1	PVC Hybrid
ATM-VISM	cbr1 vbr1_rt vbr2_rt vbr3_rt	PVC

Table 4-3 ATM (RPM) Connection and Protocol Types

Connection Type	Service Types	Protocols
ATM (RPMB)-ATM (RPMB)	vbr3_nrt abr1 ubr1	PVC Hybrid SPVC
ATM (RPMB)-Frame Relay	vbr3_nrt abr1 ubr1	PVC Hybrid SPVC
ATM (RPMB)-FUNI	vbr3_nrt abr1 ubr1	PVC Hybrid SPVC
ATM (RPMB)-Frame Forwarding	vbr3_nrt abr1 ubr1	PVC Hybrid SPVC
ATM (RPMB)-ATM	vbr3_nrt abr1 ubr1	PVC Hybrid SPVC

Table 4-4 Frame Relay Connection and Protocol Types

Connection Type	Service Types	Protocols
Frame Relay-Frame Relay	Without ForeSight With ForeSight	PVC Hybrid
Frame Relay-FUNI	Without ForeSight With ForeSight	PVC Hybrid
Frame Relay-Frame Forwarding	Without ForeSight With ForeSight	PVC Hybrid

Table 4-4 Frame Relay Connection and Protocol Types (continued)

Connection Type	Service Types	Protocols
Frame Relay-ATM	cbr1 vbr2_nrt vbr3_nrt vbr2_rt vbr3_rt abrfs ubr1 ubr2 abr1	PVC Hybrid
Frame Relay-ATM (RPMB)	vbr3_nrt abr1 ubr1	PVC Hybrid
FUNI-Frame Relay	Without ForeSight With ForeSight	PVC Hybrid
FUNI-FUNI	Without ForeSight With ForeSight	PVC Hybrid
FUNI-Frame Forwarding	Without ForeSight With ForeSight	PVC Hybrid
FUNI-ATM	cbr1 vbr2_nrt vbr3_nrt vbr2_rt vbr3_rt abrfs ubr1 ubr2 abr1	PVC Hybrid
FUNI-ATM (RPM)	vbr3_nrt	PVC Hybrid
Frame Forwarding-Frame Relay	Without ForeSight With ForeSight	PVC Hybrid
Frame Forwarding-FUNI	Without ForeSight With ForeSight	PVC Hybrid
Frame Forwarding-Frame Forwarding	Without ForeSight With ForeSight	PVC Hybrid

Table 4-4 Frame Relay Connection and Protocol Types (continued)

Connection Type	Service Types	Protocols
Frame Forwarding-ATM	cbr1 vbr2_nrt vbr3_nrt vbr2_rt vbr3_rt abrfs ubr1 ubr2 abr1	PVC Hybrid
Frame Forwarding-ATM (RPMB)	vbr3_nrt ubr1 abr1	PVC Hybrid

Table 4-5 CE Connection and Protocol Types

Connection Type	Service Types	Protocols
CE-CE	cbr1	PVC Hybrid
CE-ATM	cbr1	PVC Hybrid

Table 4-6 Voice and Data Connection and Protocol Types

Connection Type	Service Types	Protocols
Data-Data	Data	PVC
Voice-Voice	Voice	PVC

Table 4-7 VISM Connection and Protocol Types

Connection Type	Service Types	Protocols
VISM-ATM	cbr1 vbr1_rt vbr1_nrt	PVC
VISM-VISM	cbr1 vbr1_rt vbr1_nrt	PVC

Table 4-8 Private Line Connection and Protocol Types

Connection Type	Service Types	Protocols
CE-CE	cbr1	PVC Hybrid

Filter Settings

The Filter Settings feature allows you to filter connections using the following criteria: Type, Status, Multicast, Enabling Categories, Remote, Connection Descriptor, and End Point Filter Levels.

You can invoke the Filter Settings from:

- Connection Manager Main Window - select **Edit**->**Filters** menu entry. The seven filter categories are displayed in the Filter Settings Window.
- Select the desired settings and click the **OK** button.

Switch Compatibility

Release 10 of CWM can manage connections on the following types of WAN switches or concentrators:

- BPX® 8600 series wide-area switch running switch software 9.1, 9.2, or 9.3
- IGX™ 8400 series wide-area switch running switch software 9.1, 9.2, or 9.3
- MGX™ 8220 edge concentrator using firmware versions 4.0, 4.1, or 5.0
- MGX 8230 Release 1 using firmware version 10.0 (PXM1)
- MGX 8250 Release 1 using firmware version 10.0 (PXM1)
- MGX 8850 Release 1 using firmware version 10.0 (PXM1)
- MGX 8850 Release 2 using firmware version 2.0 (PXM45)
- BPX 8600 services wide-area switch running switch software 9.2.33 with BPX-SES PNNI Controller running firmware version 1.0.00, 1.0.01, or 1.0.10

Supported Cards

Release 10 of CWM supports the following card types for various connections:

Frame Relay

Service modules for Frame Relay (FR):

- FRSM (4T1,4E1,8T1,8E1), FRSM-HS1b.V35 cards for MGX 8220, MGX 8230, MGX 8250, Release 1 MGX 8850
- UFM, FRM cards in IGX

The following FRSM-VHS service modules are supported on MGX 8220, MGX 8230, MGX 8250, and Release 1 of MGX 8850:

- FRSM-2CT3
- FRSM-2T3
- FRSM-HS2B
- FRSM-2E3
- FRSM-2HS2

Both FR and FRSM-VHS service modules support the following types of ports:

- Frame Relay
- FUNI
- Frame Forwarding

Note For FRSM cards, the port information is shown as follows: **Line_number.Physical_portnumber**[**Logical_portnumber**](**PortSpeed**). The Logical port number is typically shown on the CLI when using the **dspports** command, however CWM uses the physical port number for connection provisioning.

ATM with PVC Connections

Service modules for ATM (unicast) connections:

- AUSM (4T1, 4E1, 8T1, 8E1) in MGX 8220.
- AUSM-B (8T1, 8E1) in MGX 8220, MGX 8230, MGX 8250, and Release 1 MGX 8850.
  - These cards support both ATM and IM-ATM ports.
- PXM in MGX 8850.
- ASI, ASI-155, BXM, and BXM-E in BPX.
- UXM in IGX.
- BME in BPX (only card supporting ATM multicast connections).
- RPMB in MGX 8230, MGX 8250, and Release 1 MGX 8850 (unicast connections).
- RPM-PR

Circuit Emulation (CE)

Service modules for Circuit Emulation:

- CESM-4T1 and CESM-4E1 in MGX 8220 only
- CESM-8T1 and CESM-8E1 in MGX 8230, MGX 8250, and Release 1 MGX 8850
- CESM-T3 and CESM-E3 in MGX 8230, MGX 8250, and Release 1 MGX 8850

Voice

Service modules for Voice:

- CVM and UVM in IGX

- CDP in IPX

Note IPX has been declared ‘End Of Life’ in switch software 9.1.

Data

Service modules for Data:

- HDM, LDM, UVM, CVM: IGX
- VISM 8T1/8E1

Real Time VBR Feature

Network Support

This feature is supported on network trunks running switch software 9.2.30 or later on the trunk cards BXM, BNI, UXM (only).

ATM Service Module Support

This feature is supported on the BXM, UXM, ASI service modules. Currently, CWM Release 10 does not support rt-vbr connections involving PXM cards (however PXM-FR rt-vbr connection are supported).

FR Service Module Support

This feature is supported only on FRQOS service modules.

PVC Connections Supported by Release 10 of CWM

Table 4-9 lists the Permanent Virtual Circuit (PVC) connection types supported by Release 10 of CWM.

Table 4-9 PVC Connections Types

Connection	CWM Service	Local Endpoint Card Type	Remote Endpoint Card Type	Comments or Restrictions
FR-FR	none	FR	FR	Choice of FR port types; choice of ForeSight features; no QOS support
FR-FR	none	FRQOS	FR, FRQOS	Choice of FR port types; ForeSight enabled for QOS types ubr and abr; Following QOS specified by 'ChanServType' attribute on FRSM-VHS SM: hi_priority, ubr, nrt-vbr, rt-vbr, abr
ATM-FR	nrt-vbr3,abr.fs	ATM	FR	Choice of FR port types; no QOS support on FR endpoint; abr.fs not supported with ATM PXM service module
ATM-FR	cbr1, ubr(1,2), nrt-vbr(2,3), abr.fs ubr(1,2)	ATM	FRQOS	Choice of FR port types; QOS supported on FR endpoint
ATM-FR	rt-vbr(2,3)	ATM	FRQOS	Choice of FR port types; QOS supported on FR endpoint; ForeSight for abr.fs only; abr.fs not supported with ATM PXM service module
ATM-FR	nrt-vbr3	RPMB	FR	Choice of FR port types; no QOS support on FR endpoint
ATM-FR	nrt-vbr3	RPMB	FRQOS	Choice of FR port types; QOS supported on FR endpoint
ATM-ATM	cbr1, nrt-vbr(1,2,3), ubr(1,2), abr.1,abr.fs	ATM	ATM	No Foresight (except for abr.fs); rt-vbr available only if both network and service modules support 'rt' feature; no ForeSight supported with cbr and with PXM cards
ATM-ATM	rt-vbr(1,2,3)	ATM	ATM	No Foresight; real time feature should be supported by the network and the ATM service modules
ATM-ATM	atfst. atfxt, atft-txt	ATM (BXM)	ATM (BXM)	ForeSight supported; both endpoints should be BXM/BXM-E cards
ATM-ATM	cbr1, nrt-vbr(1,2,3), ubr(1,2), abr.1,abr.fs	ATM-Multicast	ATM-Multicast	No Foresight (except for abr.fs); multicast connection; local and remote port combinations: root-root, root-leaf
ATM-ATM	nrt-vbr3 abr1 ubr1	ATM/RPM	ATM/RPM	No Foresight; one or both endpoint router service modules
VISM-ATM	cbr1 vbr1_rt vbr1_nrt	VISM	ATM	

Table 4-9 PVC Connections Types

Connection	CWM Service	Local Endpoint Card Type	Remote Endpoint Card Type	Comments or Restrictions
VISM-VISM	cbr1 vbr1_rt vbr1_nrt	VISM	VISM	
CE-CE	cbr	CE	CE	Structured/unstructured; both endpoints must be either structured or unstructured with matching bandwidth and interface type.
ATM-CE	cbr			CE structured or unstructured; ATM endpoint bandwidth should be equal to or greater than the CE endpoint bandwidth
Data-Data	none	Data service module	Data service module	Connection routing path cannot include BPX
Voice-Voice	none	Voice service module	Voice service module	Connection routing path cannot include BPX

Table 4-10 lists the cards that belong to the various endpoint card types.

Table 4-10 Card Types

Card Type	Cards
FR	FRSM(4T1,4E1,8T1,8E1, HS1b.V35), FRM, UFM, FRP
FRQOS	FRSM(2CT3,2E3,2T3,HS2) , HS2B
ATM	AUSM(4T1,4E1,8T1,8E1), AUSMB(8T1,8E1), PXM ASI, ASI-155, BXM, BXM-E, UXM (only BXM, BXM-E and UXM support rt-vbr)
ATM-Multicast	BME
CE	CESM(4T1,4E1,8T1,8E1,T3,E3)
RPMB	RPM-PR
Voice service module	CVM, UVM, CDP

Table 4-10 Card Types (continued)

Card Type	Cards
Data service module	CVM, UVM, HDM, LDM, SDP, LDP
VISM	VISM 8T1/E1

Note In this release, Multicast connections are not supported from the Connection Manager GUI.

Table 4-11 lists the cards that belong to the various endpoint card types.

Table 4-11 Card Types

Card Type	Cards
ATM (AXSM), (AXSMB)	AXSM in MGX 8850 Release 2
ATM (BXM)	BXM in BPX

Modifying Connection Parameters

From the Connection Management main window, select a node and click the **Apply** button to view connections and the status of connections on the selected node. Select a connection with a status of "O.K." Click the Modify button at the bottom of this screen to bring up a modification window for the selected connection. The new Modify Connection window displays information about the selected connection, and presents editable parameters in the far right column of the screen.

You can expand or collapse the Modify Connection and All Parameters windows by clicking the right and left arrows at the top of the screen in between these windows.

For an ATM-ATM connection with VBR Service Type, the editable connection parameters are as follows:

- Ingress UPC Parameters
  - PCR0-1(cps): Peak Cell Rate- A value that defines a rate limitation for ATM traffic used in the ingress policing algorithm. In general, traffic arriving at rates greater than the PCR are discarded.
  - CDVT0+1(usec): Cell Delay Variation Tolerance for the first leaky bucket, which applies to cells with CLP(0+1). CDVT is the maximum time for accumulated violations of cell-arrival time parameters.
  - SCR0+1(cps): Sustainable Cell Rate- The guaranteed sustainable rate for an ATM connection. Associated with the policing function used on ingress for VBR and ABR connections.
  - MBS(cells): Maximum Burst Size in cells. This is the maximum number of cells that may burst at the PCR but are still compliant. This is used to determine the Burst Tolerance (BT) which controls the time scale over which the Sustained Cell Rate (SCR) is policed..

  - Enable AAL5 FBTC: AAL5 Frame Basic Traffic Control: To enable the possibility of discarding the whole frame, not just one non-compliant cell. This is used to set the Early Packet Discard bit at every node along a connection.
  - Policing Model: When a connection is added, a VPI.VCI address is assigned, and UPC parameters are configured for the connection. For each cell in an ATM stream, the VPI.VCI addresses are verified and each cell is checked for compliance with UPC parameters.

- CAC & Rate Parameters
  - ECR Enable: Equivalent Cell Rate. The CAC (Connection Admission Control) algorithm calculates the ECR of a connection prior to establishing the connection, and ensures high efficiency of network resources.

Note If ECR is enabled, CWM will calculate %utilization using the CAC_calc.txt file. The ECR for Enhanced CAC is allowed only for BXM, ASI and AUSM cards for PVC connections. Therefore %utilization becomes a greyed out, and the user is not able to enter values in this data field.

  - Utilization(%): Is the bandwidth allocation for rt/nrt (real time/ non real time). For Vbr, Cbr, and Ubr it's PCR%Util; for Abr it's MCR%Util. Range: 0-100%.
  - MCR(cps): Minimum Cell Rate- The minimum VC queue service rate for an ABR ATM connection.

- Connection Descriptor
  - The connection descriptor is independently configurable at each end of a connection. Character Limitations: None. Range: The Descriptor field will take any number of characters, but will only display 64. To activate the Connection Descriptor feature, the following configuration steps will need to be followed. Using the command line interface (CLI) as **user svplus**:

a. **cd/usr/users/svplus/conf**

b. vi **CwmDomainGlobal.conf**

```
# Cwm Global Across the Domain Configuration File
# <Name> = <Value>
DESCRIPTOR_FLAG=0 (on=1, off=0)
```

c. Change the flag to **1** (on)

d. write and quit the file (**:wq!**)

e. Stop and restart the CWM core.

- Routing Parameters
  - Avoid Trunk Type: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
  - Reroute Priority: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
  - Enable Cell Routing: Enables Cell Routing on a connection.

- Use Trunks Using ZCS: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
- Preferred Route: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
- Override CAC: Connection Admission Control. An ATM function which determines whether a virtual circuit VC) connection request should be accepted or rejected. Override CAC allows an override option for this function.
- Route Master: The initial point of a route request.
- Current Route: The current traffic route.

Click on the parameter you would like to edit, then click on the **Edit** button at the bottom of the All Parameters window.

An Edit screen appears with all editable parameters. Make any necessary changes. Click the Apply button. All values are saved. Click **O.K.** and you are returned to the Modify Connection screen.

After applying modifications to a connection, you can save changes to a connection template for later use by clicking **Save Template**. Also, you can select **Load Template** to retrieve a previously modified connection template.

For an ATM-ATM connection with CBR Service Type, the editable connection parameters are as follows:

- Ingress UPC Parameters
  - PCR0+1(cps): Specifies the transmit/receive Peak Cell Rate (PCR) for cells leaving the first leaky bucket on the ASI card with CLP(0+1). Applies to only CBR connections. In general, traffic arriving at rates greater than the PCR are dicarded.
  - CDVT0+1(usec): Cell Delay Variation Tolerance for the first leaky bucket, which applies to cells with CLP(0+1). CDVT is the maximum time for accumulated violations of cell-arrival time parameters.
- CAC & Rate Parameters
  - CDV(usec): Cell Delay Variation. The maximum allowable delay variation through a network for a circuit emulation connection.
  - CTD(msecs): Cell Transfer Delay. The maximum delay incurred by a cell (including propagation and buffering delays.)
- Connection Descriptor
  - The connection descriptor is independently configurable at each end of a connection. Character Limitations: None. Range: The Descriptor field will take any number of characters, but will only display 64. To activate the Connection Descriptor feature, the following configuration steps will need to be followed. Using the command line interface (CLI) as **user svplus**:

a. **cd/usr/users/svplus/conf**

b. vi **CwmDomainGlobal.conf**

```
# Cwm Global Across the Domain Configuration File
# <Name> = <Value>
DESCRIPTOR_FLAG=0 (on=1, off=0)
```

c. Change the flag to **1** (on)

d. write and quit the file (**:wq!**)

e. Stop and restart the CWM core.

- Routing Parameters
  - Max Cost: Maximum cost size in cells.
  - Frame Discard: If frame-based traffic control is enabled, the EPD threshold determines when to start discarding an AAL5 frame.
  - Connection Segments: An ABR connection can be divided into separately controlled ABR segments.
- Features
  - Stats Enable: Enables statistics on a selected connection.
  - CC Enable: Congestion Control Enable. A 22-bit field in the header of the STI cell that is used to report congestion messages to the source service interface for the ForeSight feature.
- SCT Vc Parameters
  - Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
  - Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
  - Cosb Number: The Class of Service Buffer number associated with the service type. Access: read-write. Values: 1-16.
  - CAC Treatment: Connection Admission Control. The CAC algorithms that are supported are: 1) lcnCac, 2) eCac-Model A, 3) eCac-Model B, 4) eCac-Model C, 5) eCac-Model D, 6) eCac-Model E, 7) eCac-Model F, 8) mbBwCac. DEFVAL {2}. Access: read-write. Values: 1-256.
  - UPC Enable: Selectively enables or disables UPC policing on this virtual circuit. Access: read-write. Values: enableAll(1), enableGera1(2), enable Gera2(3), enable Gera1WithPktPolicing(5), enable Gera2WithPktPolicing(6).
  - UPC CLP Selection: Usage Parameter Control- Cell Loss Priority Select. Enables or disables GCRA policing functions on the connection. GCRA1-ENB: Enables GCRA1 only. GCRA 1&2: Enables both GCRA1 & GCRA2.
  - GCRA No1 Policing Action: Generic Cell Rate Algorithm- Bucket 1. In ATM an algorithm that defines conformance with respect to the traffic contract of the connection. For each cell arrival the GCRA determines whether the cell conforms to the traffic contract.
  - GCRA No2 Policing Action: Generic Cell Rate Algorithm- Bucket 2. In ATM an algorithm that defines conformance with respect to the traffic contract of the connection. For each cell arrival the GCRA determines whether the cell conforms to the traffic contract.
  - Peak Cell Rate (PCR): The peak (maximum) cell rate for a connection using this service type. This value is a percentage of the maximum cell rate for the logical interface. 1000000 is equal to 100%. Range and Units: 0-1000000.
  - Sustained Cell Rate (SCR): The sustained cell rate for a connection using this service type. This value is a percentage of the maximum cell rate for the logical interface. 1000000 is equal to 100%. Range and Units: 0-1000000.
  - Min Cell Rate (MCR): The minimum cell rate for a connection using this service type. This value is a percentage of the maximum cell rate for the logical interface. 1000000 is equal to 100%. Range and Units: 0-1000000.

- Initial Cell Rate (ICR): The cell rate used to begin a transmission on a connection that has been idle for a configured period of time. This value is a percentage of the PCR for the logical interface. 1000000 is equal to 100%. (Used only on ABR service type connections.) Range and Units: 0-1000000.
- Max Burst Size(MBS): The maximum number of cells that may arrive at a rate equal to the PCR. Used for policing. Range and Units: 1-5000000.
- Max Frame Size(MFS): The maximum AAL5 frame size in cells.
- Cell Delay Variation Tolerance(CDVT): Specifies the transmit/receive Cell Delay Variation Tolerance for the second leaky bucket. The second bucket applies to cells with CLP(0). CDVT is the maximum time for accumulated violations of cell-arrival time parameters.
- VC Packet Discard Mode: Enables or disables Packet Discard Mode on the connection. Range and units: 1=enabled; 2=disabled.
- Max Threshold: The VcMax Threshold for CLP (0+1) cells in microseconds. Range and units: 0-5000000 microseconds.
- CLP (1) High Threshold: Cell Loss Priority High Threshold (% of VC QMax) is the highest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions. Most often set by the ingress policing function.
- CLP (1) Low or EPDs (1): Cell Loss Priority Low Threshold (% of VC QMax)/ Early Packet Discard. If AAL5 FBTC = yes, then for the BXM card this is the EPD threshold setting. EPDs is the lowest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions.
- EPD Threshold: Early Packet Discard Threshold. The maximum threshold for CLP (0+1) cells. This value is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and value: 0-1000000.
- EFCI Threshold: Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.
- Class of Service Scaling: Class of Service Scaling provides a means of scaling through a set of extended parameters, which are generally platform specific, based on a set of standard ATM parameters passed to the VSI slave during connection set up.
- CI Control: Congestion Indication Control. Indicates whether the EFCI Threshold has been exceeded.
- VSVD: Virtual Source/ Virtual Destination. A VSVD is an ABR connection which may be divided into two or more separately controlled ABR segments. Each ABR control segment , except the first, is sourced by a virtual source. Sources and destinations are linked via bi-directional connections, and each connection termination point is both a source and a destination, a source for data that is transmitting, and a destination for data that is receiving.
- ACR Decrease Time Factor: Allowed Cell Rate Decrease Time Factor. Sets the Decrease Time Factor for the VC queue service rate being used on an ABR connection.
- ABR Rate Decrease Factor: Available Bit Rate-Rate Decrease Factor. Sets the Rate Decrease Factor on an ABR variable rate ATM service type utilizing the ForeSight algorithm for congestion avoidance.
- Rate Increase Factor(RIF): A percentage increase in the allowable cell rate for an ABR connection if the BRM cells do not have the N1 or C1 bits set.
- Number of Data Cells Between FRM Cells

  - Time Between Fwd RM Cells
  - Transient Buffer Exposure(TBE): The number of RM cells that can be sent out by a virtual source before waiting for a BRM cell in return.
  - Fixed Round Trip Time (in microseconds): The amount of delay expected for an RM cell to travel through the network to the destination and back again.
  - per-VC Weighted Fair Queuing (WFQ): Weighted Fair Queuing is an approximation of the Generalized Processor Sharing (GPS) scheduling. WFQ can be generally used to give performance guarantees to connections carrying best-effort packet traffic, where each connection can be guaranteed bandwidth in proportion to its weight and in a fair manner.

- SCT Cosb Parameters
  - Cosb Number: Class of Service Buffer Number. The number that identifies one of the sixteen Cosb buffers. A Cosb buffer is a buffer that services connections with similar QoS requirements. Range and units:1-16.
  - Cosb MinRate: This field is no longer used and is currently always set to its default value (0). Range and units: 1- 1000000.
  - Cosb MaxReservableRate: This field is no longer used and is currently always set to its default value (100). Range and units: 1- 1000000.
  - Min Priority: The priority at which this COSB will be serviced to guarantee it minimum and maximum bandwidth requirements. Highest priority = 0; Lowest priority = 15. Range and units: 0-15.
  - Excess Priority: The priority at which this COSB will be given access to excess bandwidth. Highest priority = 0; Lowest priority = 15. Range and units: 0-15.
  - Cosb Max Threshold: Class of Service Buffer Maximum Threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to 100%. Range and values: 0-1000000.
  - Cosb CLP (1) High Threshold: Class of Service Buffer Cell Loss Priority. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to 100%. Range and values: 0-1000000.
  - Cosb EPD (0) Threshold: Class of Service Buffer Early Packet Discard Threshold. The maximum threshold for CLP (0+1) cells. This value is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and value: 0-1000000.
  - EFCI Threshold: Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.
  - Explicit Rate Stamping: Indicates whether Explicit Rate Stamping (ERS) is enabled or disabled. Range and units: 1=enabled; 2=disabled.
  - Random Early Discard Selection(RED): RED will drop packets from queues on a random basis in order to avoid buffer overflow. RED is accomplished by dropping packets on a random basis, which is determined statistically, when the mean queue depth exceeds a threshold over a period of time, effectively advising the packet source router to decrease its packet rate.
  - Random Early Discard Threshold: The threshold at which the COSB Random Early Discard (RED) is activated. This threshold is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and units: 0-1000000.
  - Random Early Discard Probability Factor: The mantissa value of probability for maximum discard when RED is activated. Determined as 1/2^<value>.

- WFQ Enable: Weighted Fair Queuing. WFQ queues traffic in separate queues, according to traffic class definition, guaranteeing each queue some portion of the total available bandwidth. WFQ recognizes when a particular queue is not fully utilizing its allocated bandwidth and portions that capacity out to the other queues on a proportionate basis. This is done by portioning out available bandwidth on the basis of individual information flows according to their message parameters.
- Best Effort Indicator: A Quality of Service Class in which no specific traffic parameters and no absolute guarantees are provided. Best Effort includes UBR and ABR Service Types.
- Enable/disable Discard Alarm per VC: Indicates whether Discard Alarm has been enabled or disabled. Range and units: 1=enabled; 2=disabled.
- Cosb CLP (1) High Threshold: Class of Service Buffer- Cells Loss Priority High. The high hysteresis threshold at which CLP (1) cells will be discarded. The cells will continue to be discarded until the CLP_LO threshold is reached. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to 100%. Range and units: 0-1000000.

Click on the parameter you would like to edit, then click on the **Edit** button at the bottom of the All Parameters window.

An Edit screen appears with all editable parameters. Make any necessary changes. Click the Apply button. All values are saved. Click **O.K.** and you are returned to the Modify Connection screen.

After applying modifications to a connection, you can save changes to a connection template for later use by clicking **Save Template**. Also, you can select **Load Template** to retrieve a previously modified connection template.

For an ATM-ATM connection with ABR Service Type, the editable connection parameters are as follows:

- Ingress UPC Parameters
  - PCR0+1(cps): Peak Cell Rate- A value that defines a rate limitation for ATM traffic used in the ingress policing algorithm. In general, traffic arriving at rates greater than the PCR are discarded.
  - CDVT0+1(usec): Cell Delay Variation Tolerance for the first leaky bucket, which applies to cells with CLP(0+1). CDVT is the maximum time for accumulated violations of cell-arrival time parameters.
  - MBS(cells): Maximum Burst Size in cells. This is the maximum number of cells that may burst at the PCR but are still compliant. This is used to determine the Burst Tolerance (BT) which controls the time scale over which the Sustained Cell Rate (SCR) is policed.
  - Enable AAL5 FBTC: AAL5 Frame Basic Traffic Control: To enable the possibility of discarding the whole frame, not just one non-compliant cell. This is used to set the Early Packet Discard bit at every node along a connection.
  - Policing Model: Available Bit Rate (ABR) connections are policed in the same manner as the Vbr connections, but in addition use either the ABR Standard with VSVD congestion flow control method or the ForeSight option to take advantage of unused bandwidth when it is available.
- CAC & Rate Parameters
  - Utilization (%): Is the bandwidth allocation for rt/nrt (real time/ non real time). For Vbr, Cbr, and Ubr it's PCR%Util; for Abr it's MCR%Util. Range: 0-100%.
  - MCR(cps): Minimum Cell Rate. A minimum cell rate committed for delivery by the network.
  - ICR(cps): Initial Cell Rate. The rate at which a source should send initially and after an idle period. MCR-PCR cells per second.

  - Rate Up: Specifies the increment in cell rate when the rate goes up. The Foresight Rate Up increment is in cells per second per adjustment
  - Rate Down: Specifies large reductions in the transmit/receive cell rate. This ForeSight Rate Down value is a percentage of the current rate.
  - ADTF/IcrTimeout(millisec): Allowed-cell-rate Decrease Time Factor/Initial-cell-rate Time-out. The time between RM cells before the allowable cell rate returns to the initial cell rate.
  - TRM/MinAdjust Period(millisec): Time RM/Minimal Adjustment Period. The maximum amount of time between RM cells on an ABR connection.

- Connection Descriptor
  - The connection descriptor is independently configurable at each end of a connection. Character Limitations: None. Range: The Descriptor field will take any number of characters, but will only display 64. To activate the Connection Descriptor feature, the following configuration steps will need to be followed. Using the command line interface (CLI) as **user svplus**:

a. **cd/usr/users/svplus/conf**

b. vi **CwmDomainGlobal.conf**

```
# Cwm Global Across the Domain Configuration File
# <Name> = <Value>
DESCRIPTOR_FLAG=0 (on=1, off=0)
```

c. Change the flag to **1** (on)

d. write and quit the file (**:wq!**)

e. Stop and restart the CWM core.

- Routing Parameters
  - Avoid Trunk Type: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
  - Reroute Priority: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
  - Enable Cell Routing: Enables Cell Routing on a connection.
  - Use Trunks Using ZCS: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
  - Preferred Route: This type is applicable only when a connection involves multiple routing nodes. Routing is not involved when a connection originates and terminates on the same routing node. That is, when originating and terminating endpoints are using the same routing node, this parameter is not applicable and is made insensitive. (Greyed out).
  - Override CAC: Connection Admission Control. An ATM function which determines whether a virtual circuit VC) connection request should be accepted or rejected. Override CAC allows an override option for this function.
  - Route Master: The initial point of a route request.
  - Current Route: The current traffic route.

- UPC Thresholds
  - Hi CLP(% of VCQ): Cell Loss Priority High Threshold (% of VC QMax) is the highest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions. Most often set by the ingress policing function.
  - Lo CLP(% of VCQ): Cell Loss Priority Low Threshold (% of VC QMax) is the lowest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions.
  - Vc Queue size (VCQ): A FIFO (First In First Out) buffer that is created for each connection when the connection is added. VC_Queue has configurable thresholds for EFCI, CLP Hi, CLP Lo. For ABR connections, cells move from VC_Queues to QBINs at the Allowed Cell Rate (ACL) as determined by the ATM Forum ABR algorithm or the Cisco Foresight algorithm.
  - EFCI Queue Size(% of VCQ): Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.
- Flow Control Service
  - Enable BCM: Backward Congestion Management.
  - Enable VSVD: Virtual Source/ Virtual Destination. A VSVD is an ABR connection which may be divided into two or more separately controlled ABR segments. Each ABR control segment, except the first, is sourced by a virtual source. Sources and destinations are linked via bi-directional connections, and each connection termination point is both a source and a destination, a source for data that is transmitting, and a destination for data that is receiving. The forward direction is defined as from source to destination, and the backward direction is defined as from destination to source. Enable VSVD enables this Flow Control Service.
  - NRM(cells): Number RM. The maximum number of data cells that can be sent before sending an RM cell on an ABR connection.
  - TBE(cells): Transient Buffer Exposure. The number of RM cells that can be sent out by a virtual source before waiting for a BRM cell in return.
  - FRTT(millisec): Fixed Round-Trip Time. The amount of delay expected for an RM cell to travel through the network to the destination and back again.

Click on the parameter you would like to edit, then click on the **Edit** button at the bottom of the All Parameters window.

An Edit screen appears with all editable parameters. Make any necessary changes. Click the Apply button. All values are saved. Click **O.K.** and you are returned to the Modify Connection screen.

After applying modifications to a connection, you can save changes to a connection template for later use by clicking **Save Template**. Also, you can select **Load Template** to retrieve a previously modified connection template.

XPVC Supported Connections

Autoroute one/two/three segment PVC can be transformed to two/three segment XPVC in two stages: deletion of PVC & addition of SPVC. The SPVC of the resulting XPVC will replace/substitute/extend one of the **routing** PVC leg of the original PVC multi-segment connection.

Note XPVC connections can only be added by a proxy; not GUI.

For the ATM - ATM (AUSM-AUSM 3 segment, BXM - BXM 1 segment) PVC & SPVC routing segment is same for all ATM service types: cbr, rt-vbr, nrt-vbr, ubr, abrstd, abrfst.

For the FR - FR (FRSM-FRSM 3 segment), with atfr PVC middle segment, the SPVC segment type is nrt-VBR.

For the FR - FR with foresight (FRSM-FRSM 3 segment) PVC, with atfst PVC middle segment, the SPVC segment type is abrstd.

For the ATM (cbr, rt-vbr, nrt-vbr, ubr) - FR (FRSM - BXM 2 segment, AUSM - FRSM 3 segment) PVC, the middle/routing segment is the same ATM type SPVC.

For the ATM (abrfst) - FR (FRSM - BXM 2 segment, AUSM - FRSM 3 segment) PVC, the middle/routing segment is abrstd SPVC.

For the ATM - FR with foresight (atfst) PVC routing segment (only 2 segment supported) the middle/routing segment is abrstd SPVC.

For the RPM-RPM (3 segment), RPM-ATM (2 or 3 segment), RPM-FR (2 or 3 segment) nrt-VBR3/ubr1/abr1, the middle segment is nrt-VBR3/ubr1/abr1.

Note ABRFST is not supported in SPVC model; these connections are converted to Standard ABR.

Table 4-12 lists Three Segment XPVC services and segments.

Table 4-12 Three Segment XPVC

XPVC Service	AR Feeder Segment 1	AR Routing Segment 1	PNNI Routing Segment	AR Routing Segment 2	AR Feeder Segment 2
ATM- CBR, rt-VBR, nrt-VBR, UBR	ATM	ATM	ATM	ATM	ATM
ABRFS - ABRFS	ABRFST	ABRFST	ABRSTD without VsVd	ABRFST	ABRFST
ABRSTD - ABRSTD	ABRSTD with Termination	ABRSTD without VsVd	ABRSTD without VsVd	ABRSTD without VsVd	ABRSTD with Termination
ABRFS - ABRSTD	ABRFST	ABRFST with FCES	ABRSTD without VsVd	ABRSTD without VsVd	ABRSTD with Termination
FR-FR	FR	ATFR	nrt-VBR	ATFR	FR
FR-FR with Foresight	FST	FST	ABRSTD without VsVd	FST	FST
ATM-FR	ATFR	ATFR	ATM (CBR,rt-VBR, nrt-VBR, UBR)	ATFR	ATFR
ATM-FR Foresight	ATFST	ATFST	ABRSTD without VsVd	ATFST	ATFST
ATM-RPM nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1

Table 4-12 Three Segment XPVC (continued)

XPVC Service	AR Feeder Segment 1	AR Routing Segment 1	PNNI Routing Segment	AR Routing Segment 2	AR Feeder Segment 2
ATM-RPM abr1	abr1 with termination	abr1 w/o VSVD	abr1	abr1 w/o VSVD	abr1 with termination
RPM/ RPM-PR - RPM/RPM-PR nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1
RPM/ RPM-PR - RPM/RPM-PR abr1	abr1 with termination	abr1 w/o VSVD	abr1	abr1 w/o VSVD	abr1 with termination
RPM/ RPM-PR - FR nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1
RPM/ RPM-PR - FR abr1	abr1 with termination	abr1 w/o VSVD	abr1	abr1 w/o VSVD	abr1 with termination

Various AR PVC endpoints are listed in Table 4-13.

Table 4-13 Two Segment XPVC

XPVC Service	AR Feeder Segment	AR Segment	PNNI Routing Segment	PNNI Feeder Segment
ABR - ABRFS	ABRFST	ABRFST with FCES	ABRSTD without VsVd	ABRSTD with Termination
ATM-FR	ATFR	ATFR	ATM (CBR, rt-VBR, nrt-VBR, UBR)	ATM (CBR, rt-VBR, nrt-VBR, UBR)
ATM-FR Foresight	ATFST	ATFST with FCES	ABRSTD without VsVd	ABRSTD with Termination
ATM-RPM nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1

Table 4-13 Two Segment XPVC (continued)

XPVC Service	AR Feeder Segment	AR Segment	PNNI Routing Segment	PNNI Feeder Segment
ATM-RPM abr1	abr1 with termination	abr1 w/o VSVD	abr1	abr1 with termination
RPM/ RPM-PR - RPM/RPM-PR nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1
RPM/ RPM-PR - RPM/RPM-PR abr1	abr1 with termination	abr1 w/o VSVD	abr1	abr1 with termination
RPM/ RPM-PR - FR nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1	nrt-VBR3/ubr1
RPM/ RPM-PR - FR abr1	abr1 with termination	abr1 w/o VSVD	abr1	abr1 with termination

SPVC & PVC parameters for a Newly Established XPVC

All the AR and PNNI common parameters are provided by users. The SCT fields for AXSM assigned values are as per recommendation.

XPVC Connection and Segments

The following **XPVC Connection and Segments** window, as shown in Figure 4-3, appears after a XPVC connection has been selected from the list of connections in the Connection Manager main window, and after **XPVC Segments** has been selected from the **View** pulldown menu on the CWM main menu bar. The **XPVC Connection and Segments** window can also be opened by right clicking on the main window.

Figure 4-3 XPVC Connection and Segments

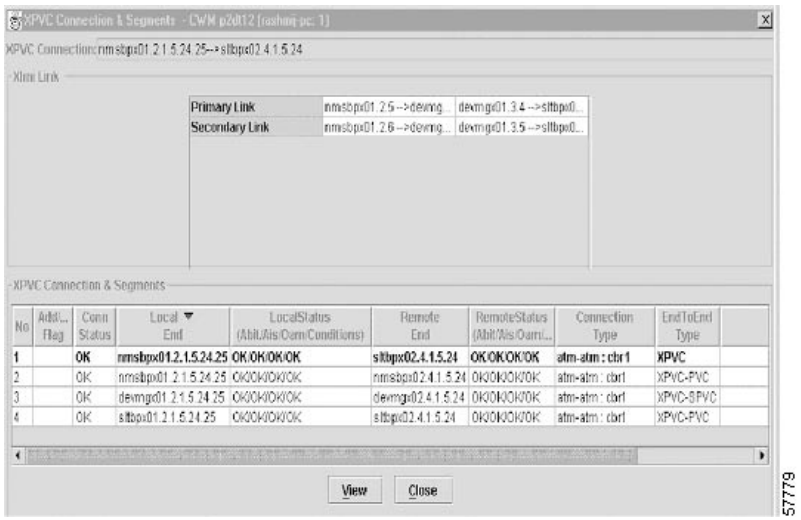
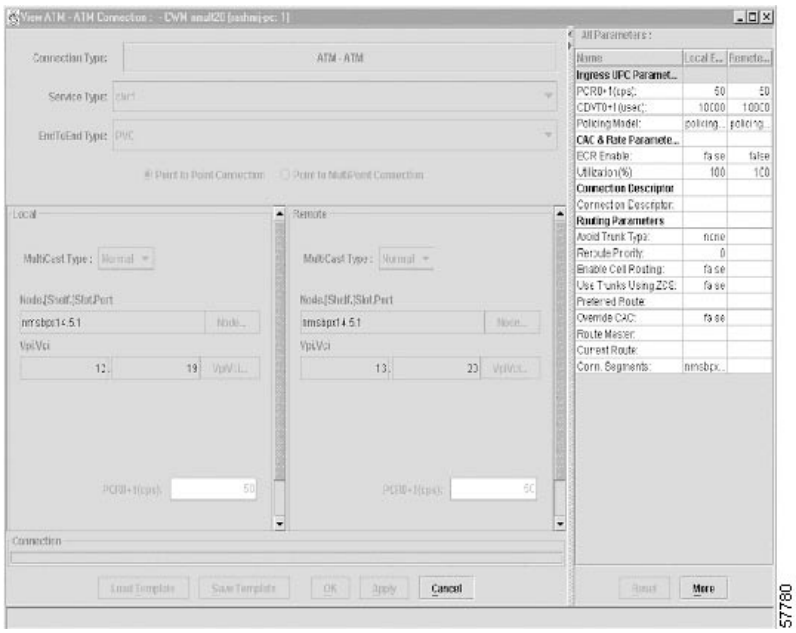


Figure 4-4 shows a new ATM-ATM Connection window.

Figure 4-4 ATM to ATM Connection



Note The VCI can be an asterick (*) to indicate the connection is a *virtual path connection* (so the VCI has no meaning within the network). The VCI range is 1-65535.

Figure 4-5 shows the Filter settings dialog box with End to End type and Dangling Segments of XPVC selected.

Figure 4-5 Filter Settings, Dangling Segments of XPVC

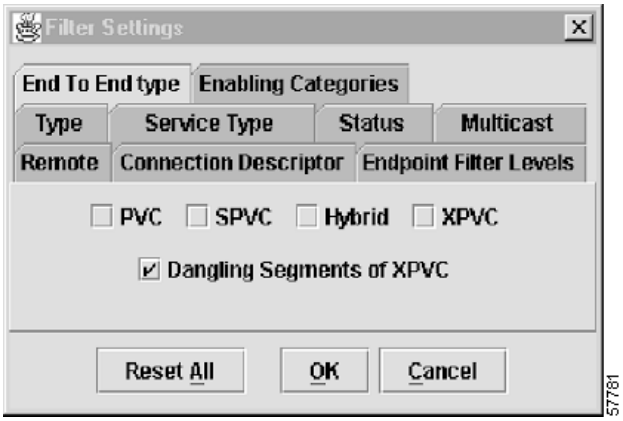
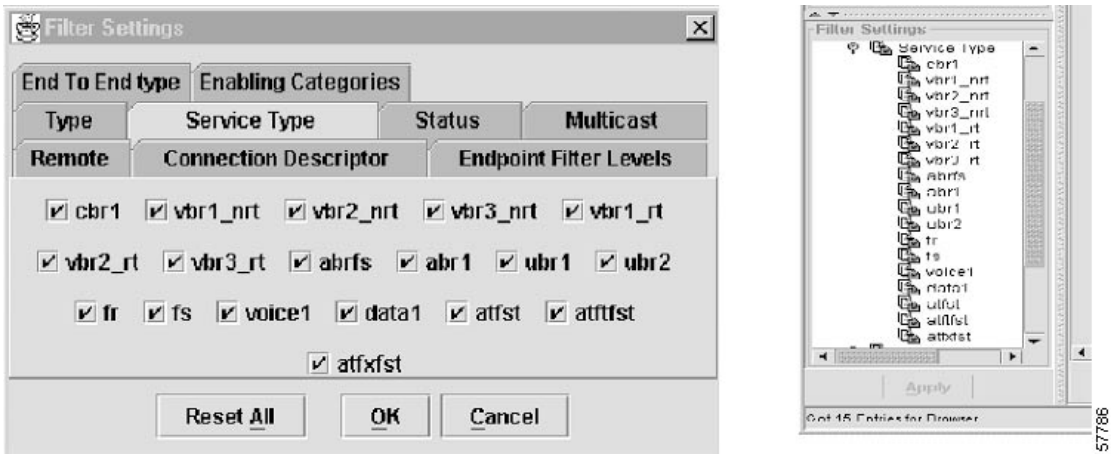


Figure 4-6 shows the Filter settings dialog box with available Service Types selected.

Figure 4-6 Filter Settings Service Type



CHAPTER 5

Network Browser

This chapter describes how to use the Network Browser application, which is launched from the CWM desktop. The Network Browser application provides a hierarchical representation of network elements, including networks, nodes, cards, lines and ports, displayed in tree format in the left panel of the Network Browser's main window. Associated information about a selected network element is displayed in table format in the right panel of the Network Browser window.

Each network element managed by Cisco WAN Manager (CWM) has its own attributes and fits into the network's physical or logical hierarchy. In Release 10 of CWM, the Network Browser presents the network elements that are discovered, managed, and controlled in a hierarchical view for all networks populated in the tables by CWM processes.

The Network Browser displays the network elements in a hierarchical format based on either a physical or logical relationship among the various network elements. Networks are displayed at the root level of the component tree, and nodes and trunks are displayed beneath the networks in a parent/child relationship.

The Network Browser also displays informational messages in a multi-line text display; other types of messages can be displayed in response to user actions.

Launching the Network Browser

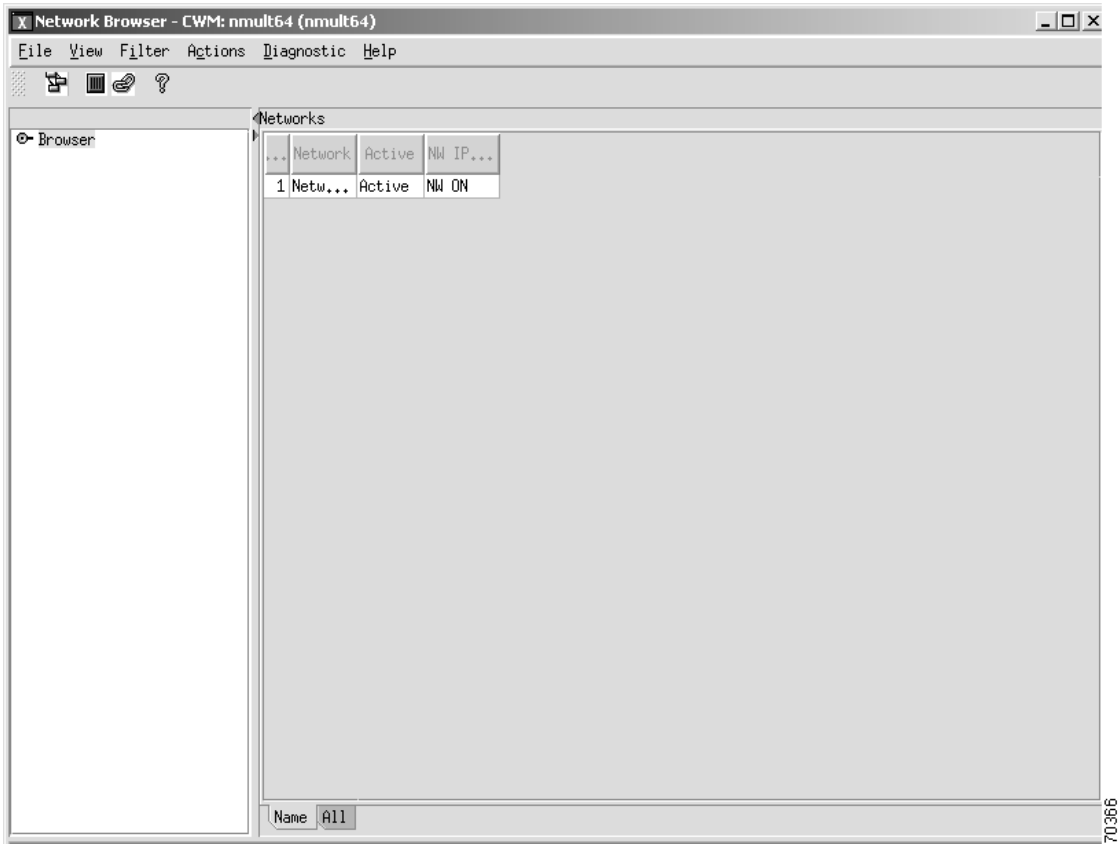
To launch the Network Browser application, click on the Network Browser icon, which is found on the Network Topology tool bar, or select the Network Browser application from the **Apps** pull-down menu located on the main menu bar.

Note Updates will not be reflected in the Network Browser if the CWM core is not running.

Main Window

After launching the Network Browser application for the first time, you will see a root node called Browser in the left panel of the window, and discovered networks in the right panel of the window in table format, as shown in Figure 5-1.

Figure 5-1 Network Browser Main Window

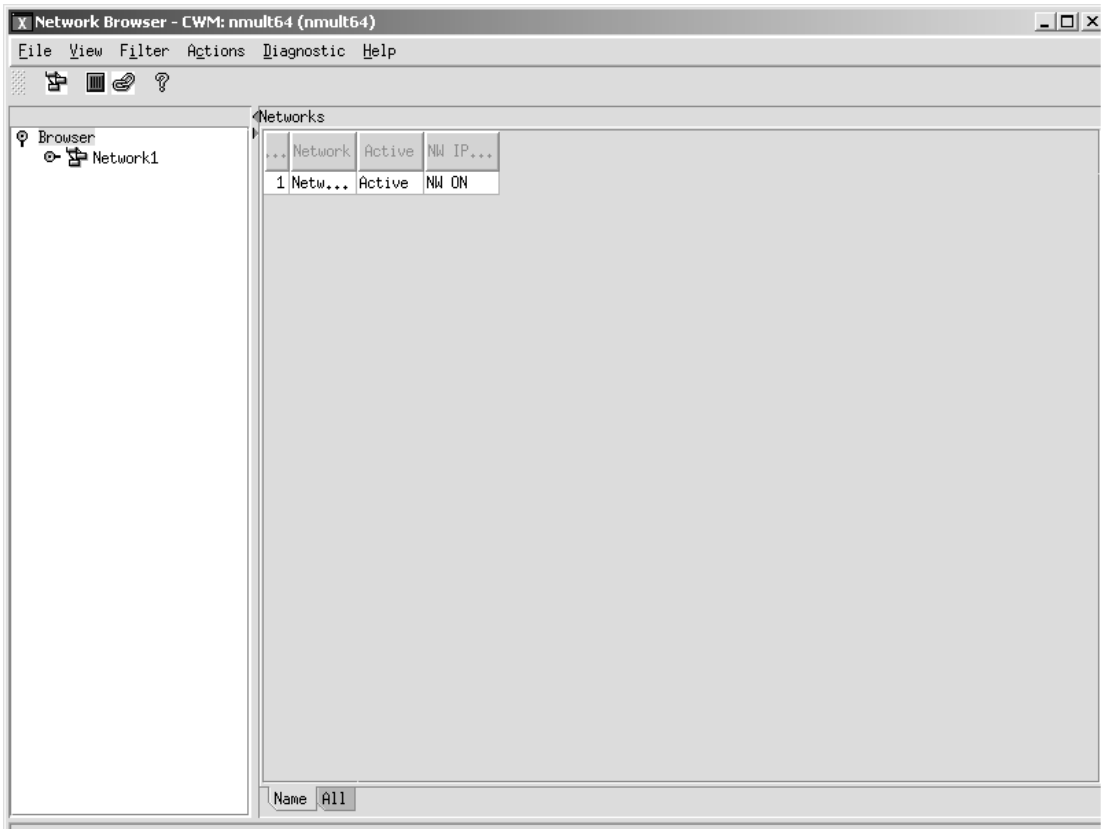


When you click on the eye glass to the left of the Browser root node, the CWM application fetches all available networks in the database and displays them in the left panel of the window. Network information will be listed in table format in the right panel of the window. This table includes the network number, network name, active or inactive status, and NW IP status.

Note The NWIP flag is not applicable to PNNI nodes.

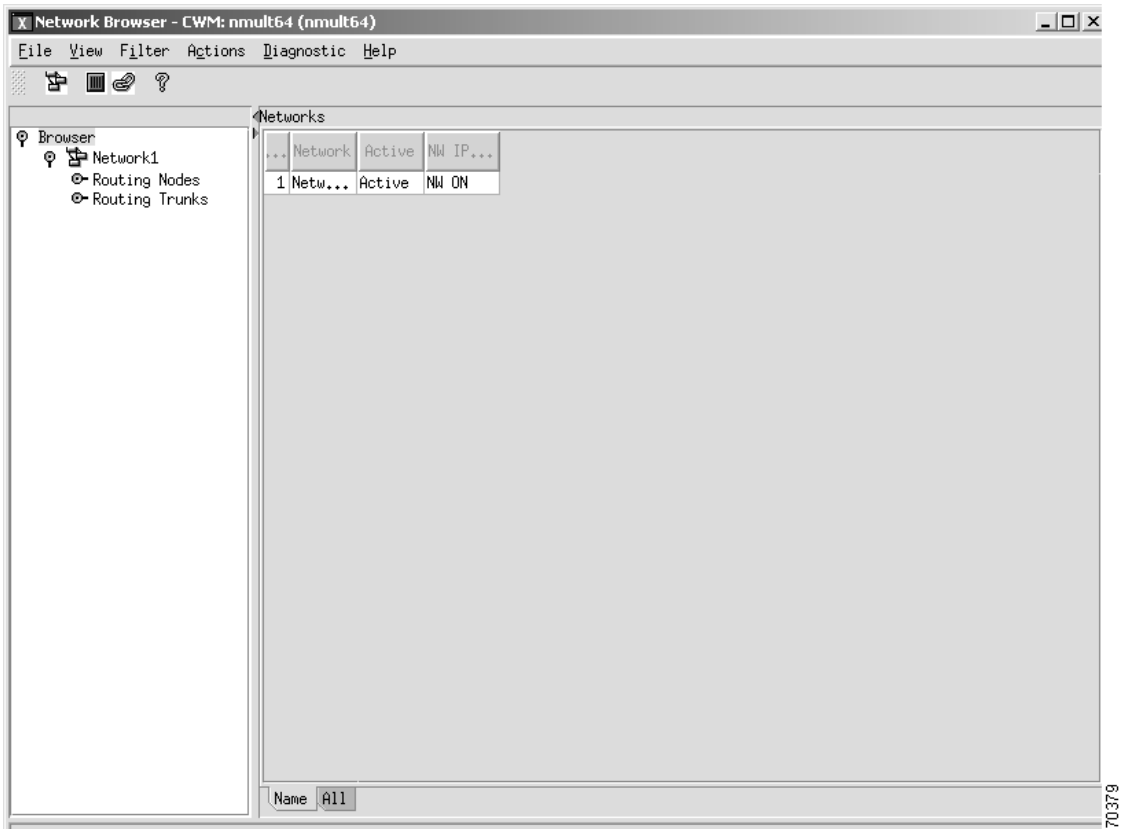
In Figure 5-2, Network 1 appears after clicking on the eye glass to the left of the Browser root node.

Figure 5-2 Network Browser Root Node Expanded



The network elements contained in Network 1 appear after clicking on the eye glass to the left of Network 1, as shown in Figure 5-3, where Routing Nodes and Routing Trunks are displayed.

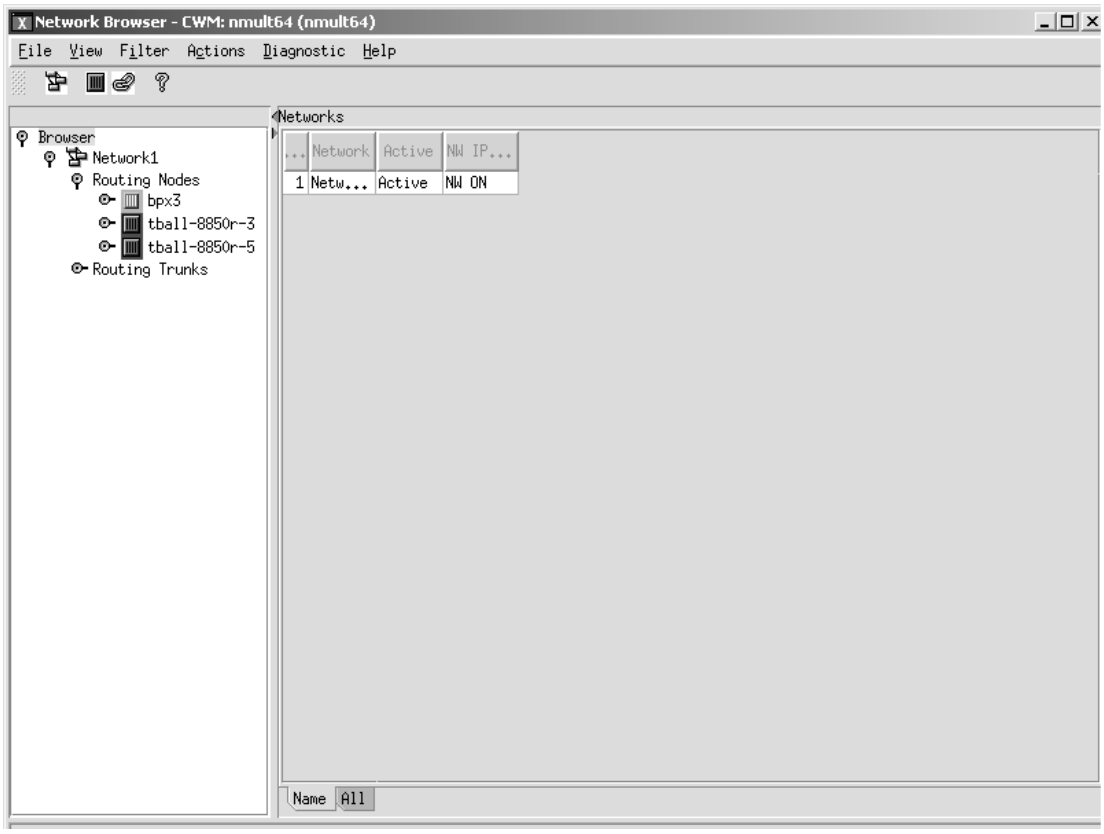
Figure 5-3 Routing Nodes and Routing Trunks



Routing Nodes

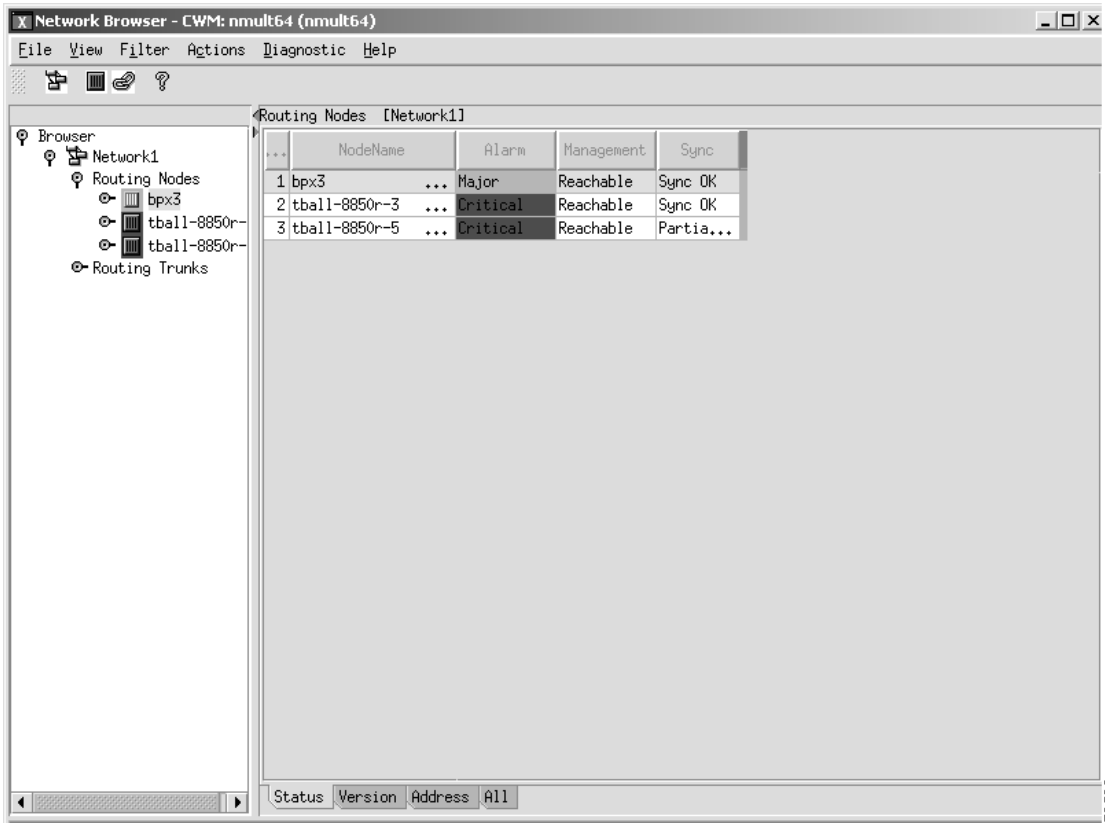
Click on the eye glass to the left of Routing Nodes to display the corresponding network elements, as shown in Figure 5-4.

Figure 5-4 Routing Nodes Expanded in Left Panel of Window



In Figure 5-5, the routing node called bpx3 has been selected, and its corresponding information appears in the right panel of the window.

Figure 5-5 Routing Node Information Displayed in Right Panel of Window



Status information for the selected routing node is indicated by the default **Status** tab at the bottom of the Network Browser window, and includes the node number, node name, alarm status, management status and synchronization status.

Click on the **Version** tab to display additional information about the selected routing node, including the node number, node name, node type, revision and protocol.

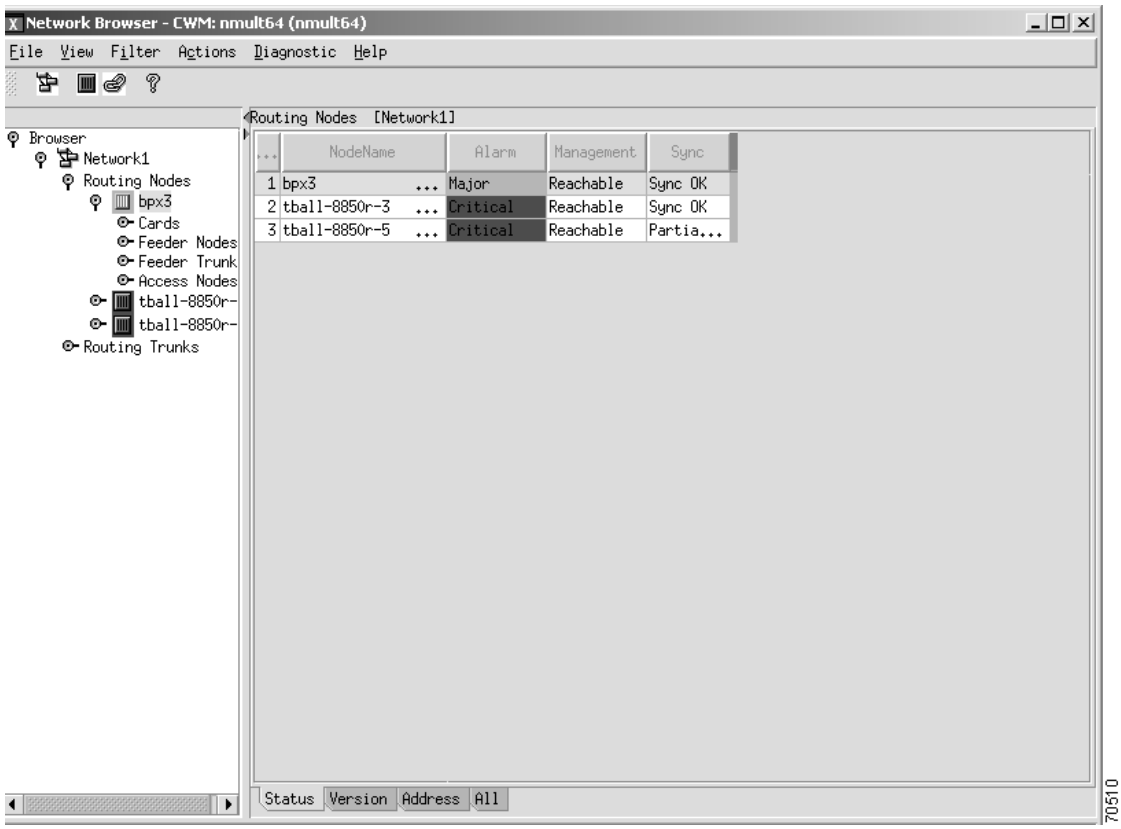
Click on the **Address** tab to display additional information about the selected routing node, including the node number, node name, LAN IP address and Network IP address.

Click on the **All** tab to display additional information on all of these categories in one screen.

Click on the eye glass to the left of the routing node to display the corresponding network elements, as shown in Figure 5-6, where the bpx3 routing node has been selected and cards, feeder nodes, feeder trunks and access nodes are displayed as network elements.

Note CWM uses color to display alarm situations detected by the Network Browser.

Figure 5-6 Routing Node's Network Elements



Cards

Click on the eye glass to the left of Cards and an expanded view of all cards for the selected routing node will be displayed in the left panel of the window, as shown in Figure 5-7. When you select a card from the left panel of the window, as shown in Figure 5-8, information about the card is displayed in the right panel of the window in table format. The right panel displays information according to the selected tab located at the bottom of the window: **Type**, **Revision**, **Redundancy Info** and **All**, as described shortly. Use the horizontal scroll bar, located at the bottom of both panels, to view undisplayed columns.

Cards Table Type information is listed in Table 5-1.

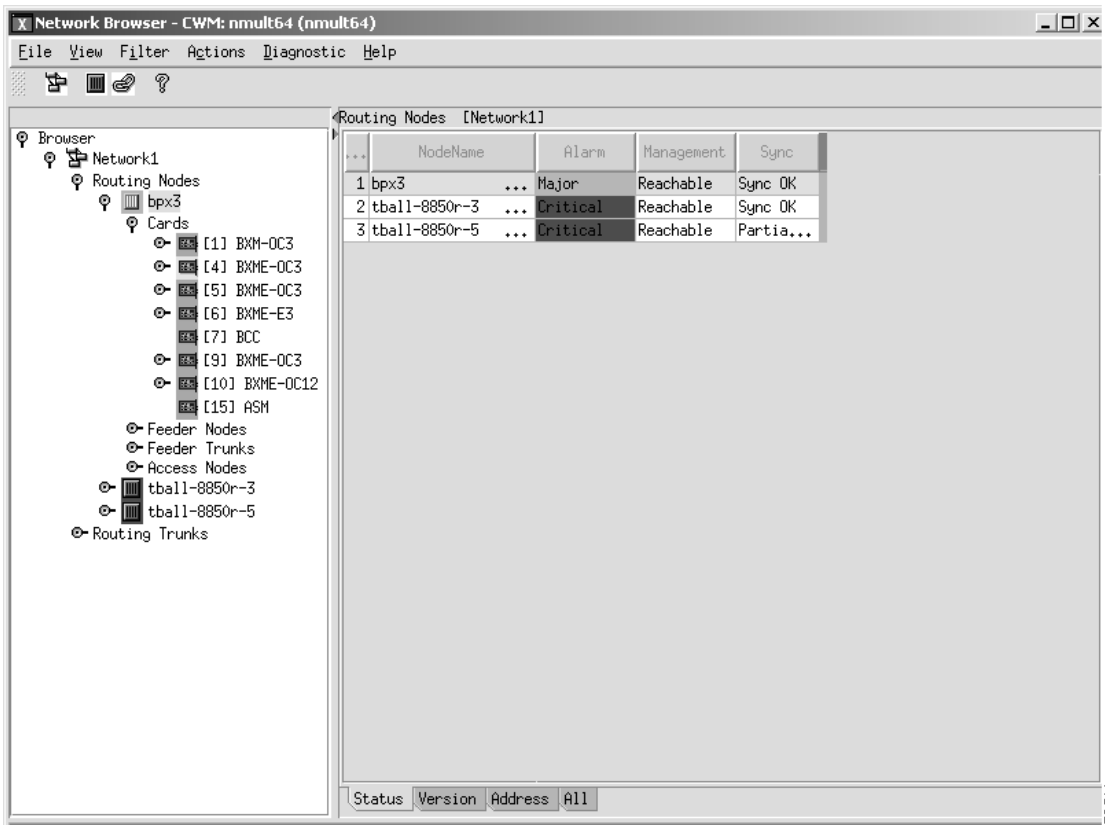
Table 5-1 Cards Table- Type Information

Column Heading	Meaning
Name	Card format *card:line:port*
Logical Slot	Logical card slot
Alarm State	Card alarm status shown in text and color Active (green) Standby (yellow)

Table 5-1 Cards Table- Type Information

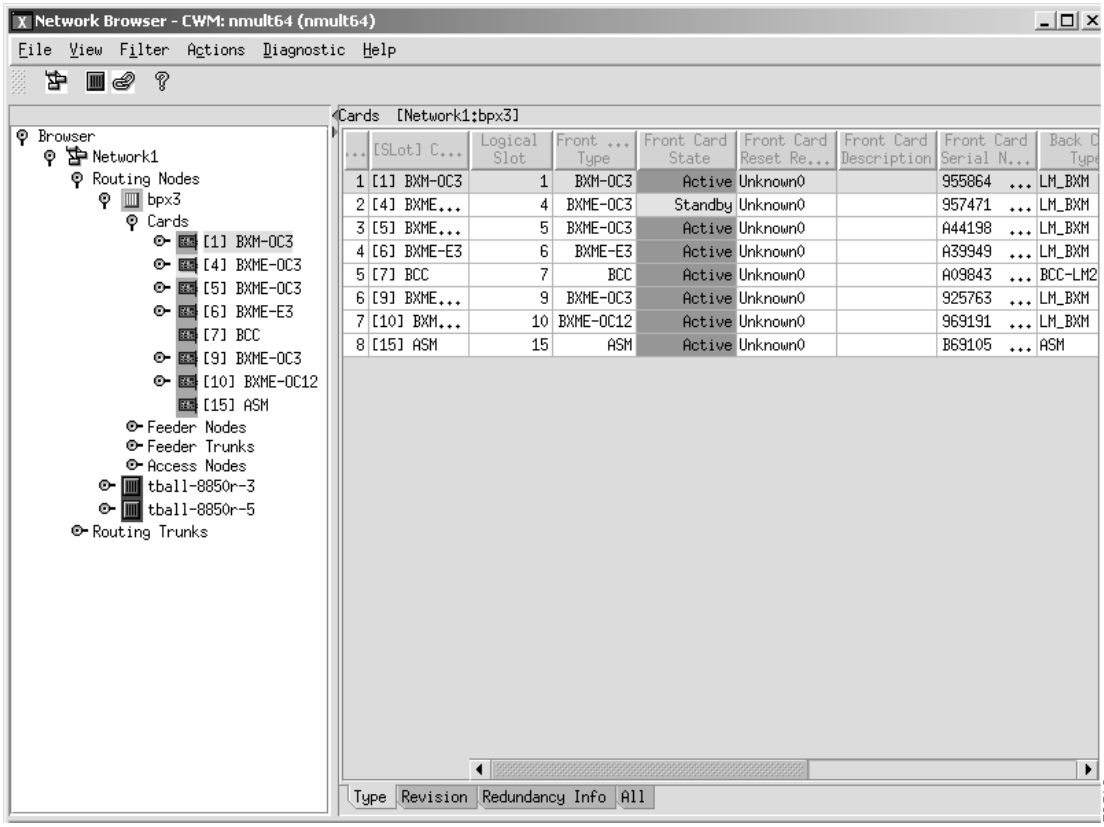
Column Heading	Meaning
Back Card	Back Card
Second Back Card	Back Card

Figure 5-7 Cards for a Selected Node Displayed in the Left Panel



Select a card to display the corresponding information about the card in the right panel of the window, as shown in Figure 5-8.

Figure 5-8 Information for a Selected Card Displayed in the Right Panel



Type information for the selected card is indicated by the default **Type** tab located at the bottom of the Network Browser window, and includes card slot and card name, logical slot, front card type, front card state, front card reset reason, front card description, front card serial number, back card type, back card state, back card description, back card serial number, second back card type, second back card state, second back card description and second back card serial number.

Click on the **Revision** tab to display additional information about the selected card, including card slot and card name, front card hardware revision, front card firmware revision, back card hardware revision, back card firmware revision, second back card hardware revision and second back card firmware revision.

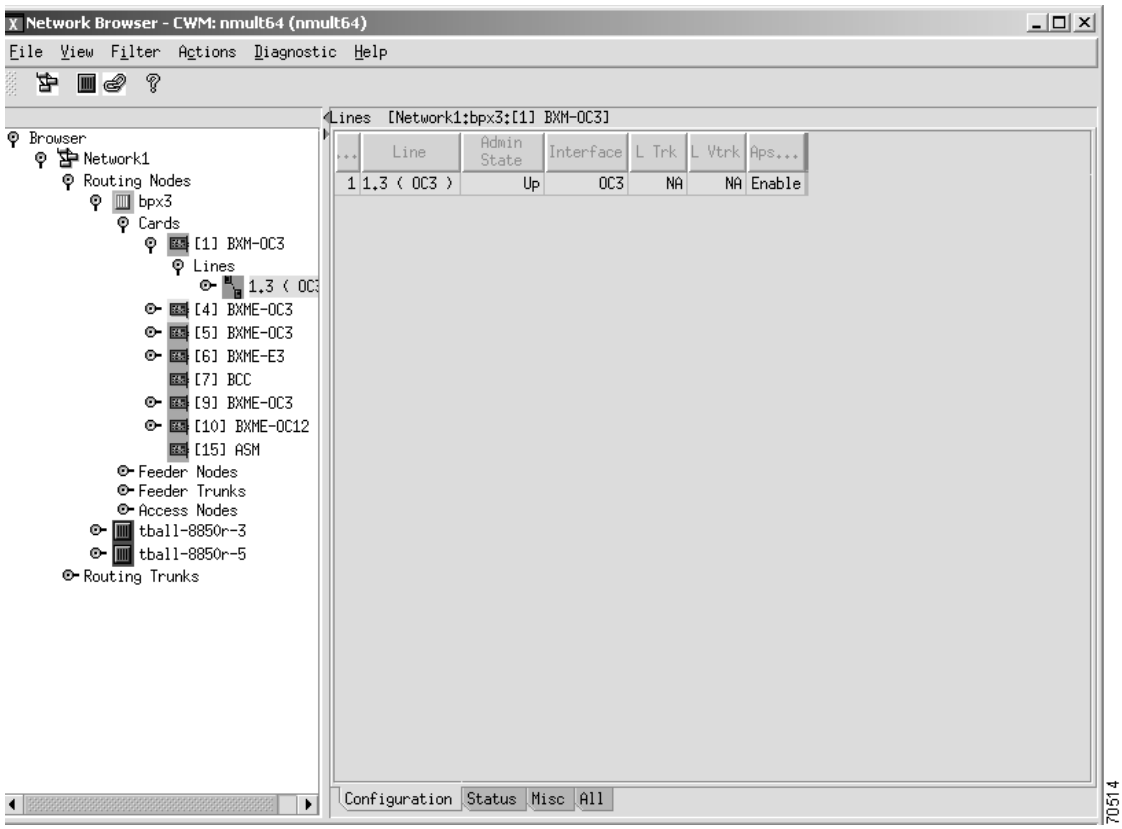
Click on the **Redundancy Info** tab to display additional information about the selected card, including card slot and card name, primary card type and slot, primary card status, secondary card type and slot, secondary card status, covered slot and redundancy type.

Click on the **All** tab to display additional information on all of these categories in one screen.

Lines

Click on the eyeglass to the left of any of the listed cards to display lines; click on the eye glass to the left of a listed line to display the corresponding information about the line in the right panel of the window. Figure 5-9 shows a line for a selected card expanded in tree format in the left panel of the window, and the corresponding information for the selected line displayed in table format in the right panel of the window.

Figure 5-9 Line Information



Configuration information for the selected line is indicated by the default **Configuration** tab located at the bottom of the Network Browser window, and includes line number, admin state, interface, trunk, virtual trunk and aps flag.

Click on the **Status** tab to display additional information about the selected line including line number, interface and alarm status.

Click on the **Misc** tab to display additional information about the selected line including line number, interface and miscellaneous comments.

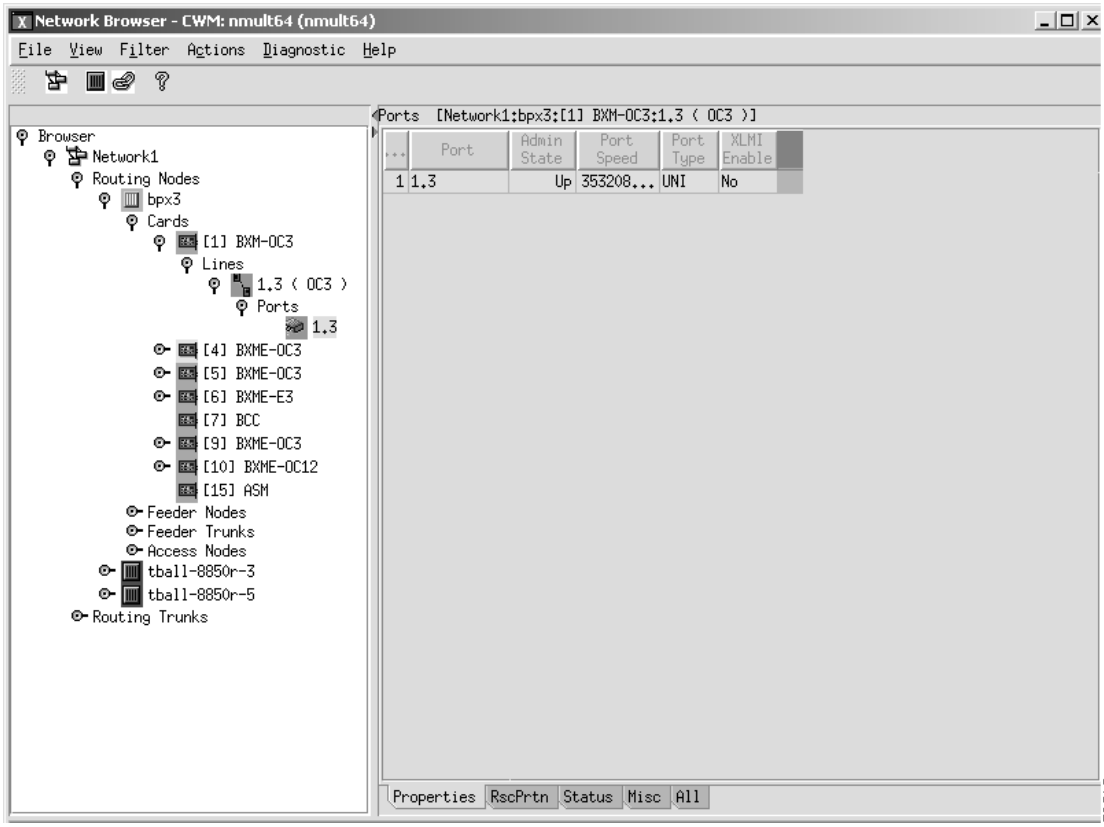
Click on the **All** tab to display additional information on all of these categories in one screen.

Ports

Click on the eyeglass to the left of a selected line to display ports; click on the eye glass to the left of Ports to display ports. Highlight a port and the corresponding information about the port will be displayed in the right panel of the window. Figure 5-10 shows a port for a selected card on a BPX node expanded in tree format in the left panel of the window, and the corresponding information for the selected port presented in table format in the right panel of the window.

Note Information displayed in the right panel of the Network Browser window for a selected port on a BPX node is different from the information displayed for other types of nodes.

Figure 5-10 Port Information



For BPX nodes, properties for the selected port is indicated by the default **Properties** tab located at the bottom of the Network Browser window, and includes slot.port, admin state, port speed and whether the port is XLMI enabled.

Click on the **RscPrtn** tab to display additional information about the selected port including the slot.port, part ID, Ctlr type, egress and ingress guaranteed and maximum bandwidths, minimum and maximum vpi and vci, minimum and maximum connections and channels, and ingress and egress percent bandwidth.

Click on the **Status** tab to display additional information about the selected port including slot.port and port status.

Click on the **Misc** tab to display additional information about the selected port including slot.port and miscellaneous comments.

Click on the **All** tab to display additional information on all of these categories in one screen.

For nodes *other than* BPX nodes, configuration information for the selected port is indicated by the default **Configuration** tab located at the bottom of the Network Browser window, and includes slot.line.port, admin state, guaranteed and maximum bandwidth, interface type, port SCT ID, SCT version, VPI #, IF index, port speed, high speed, signal state, IMA port, line map, # of redundancy links, maximum delay, IMA master, local and remote IMA ID, line order, IMA symmetry and XLMI information.

Click on the **RscPrtn** tab to display additional information about the selected port including the slot.line.port, ingress guaranteed and maximum bandwidth, minimum and maximum vpi and vci, minimum connections, maximum connections, minimum channels, maximum channels, ingress and egress percent bandwidth.

Click on the **Status** tab to display additional information about the selected port including slot.line.port and port status.

Click on the **Misc** tab to display additional information about the selected port including slot.port and miscellaneous comments.

Click on the **All** tab to display additional information on all of these categories in one screen.

To view information about other routing nodes in the network, click on the eye glass to the left of feeder nodes, feeder trunks or access nodes to display the corresponding network elements; select an element and the corresponding information will be displayed in the right panel of the window. Figure 5-11 shows a selected feeder node in the left panel of the window, and its corresponding information in the right panel of the window.

Figure 5-11 Feeder Nodes

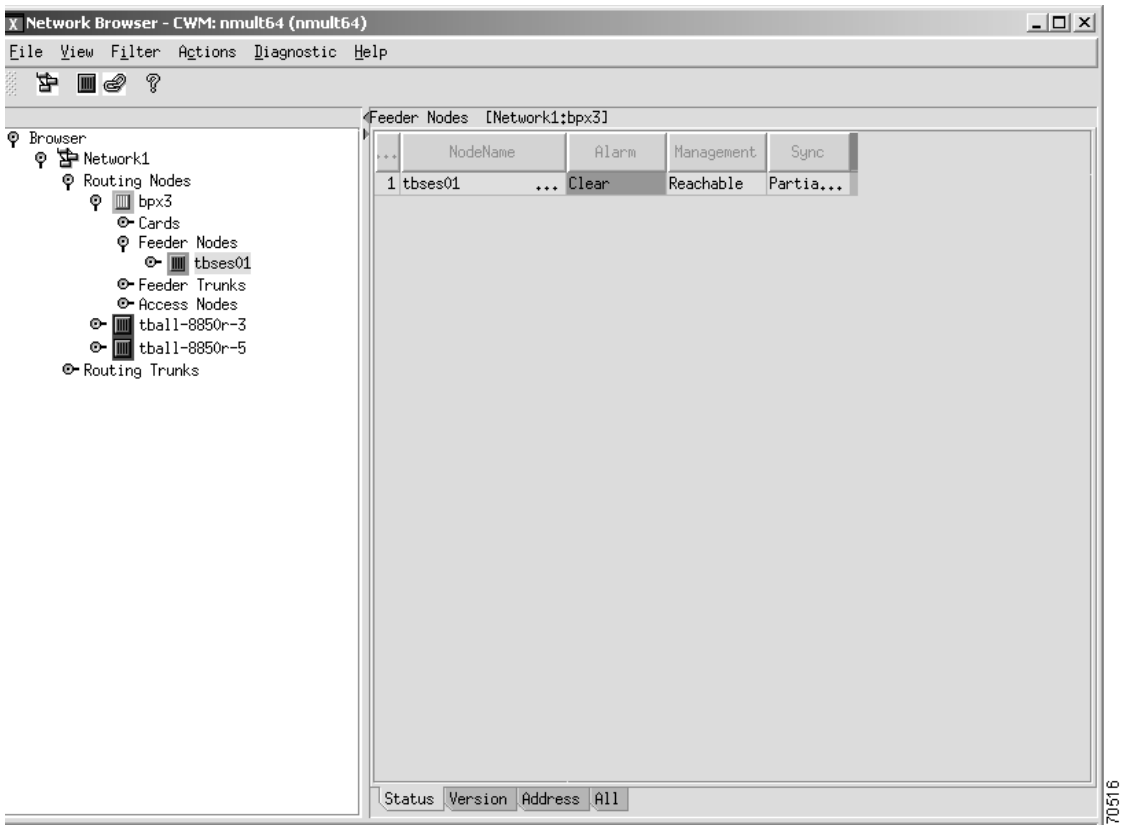


Figure 5-12 shows network elements for the selected feeder node expanded in tree format in the left panel of the window. Select a network element to display its corresponding information in the right panel of the window.

Figure 5-12 Feeder Node's Network Elements

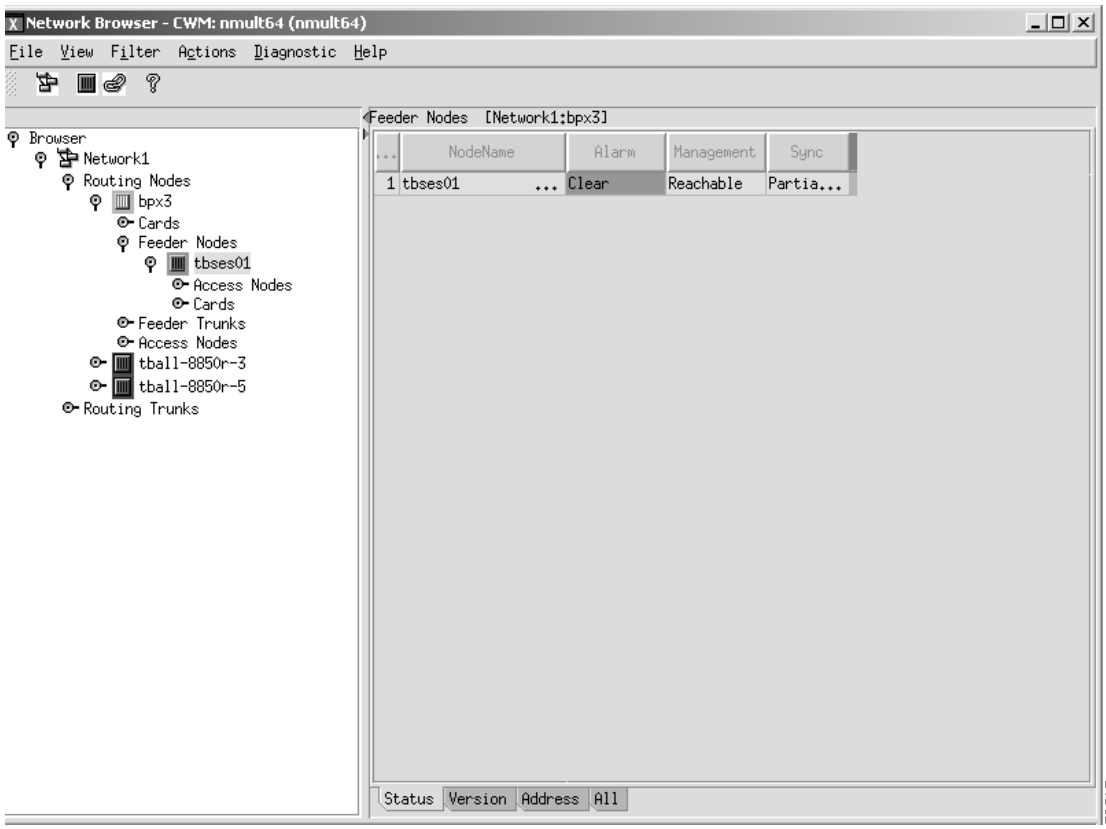
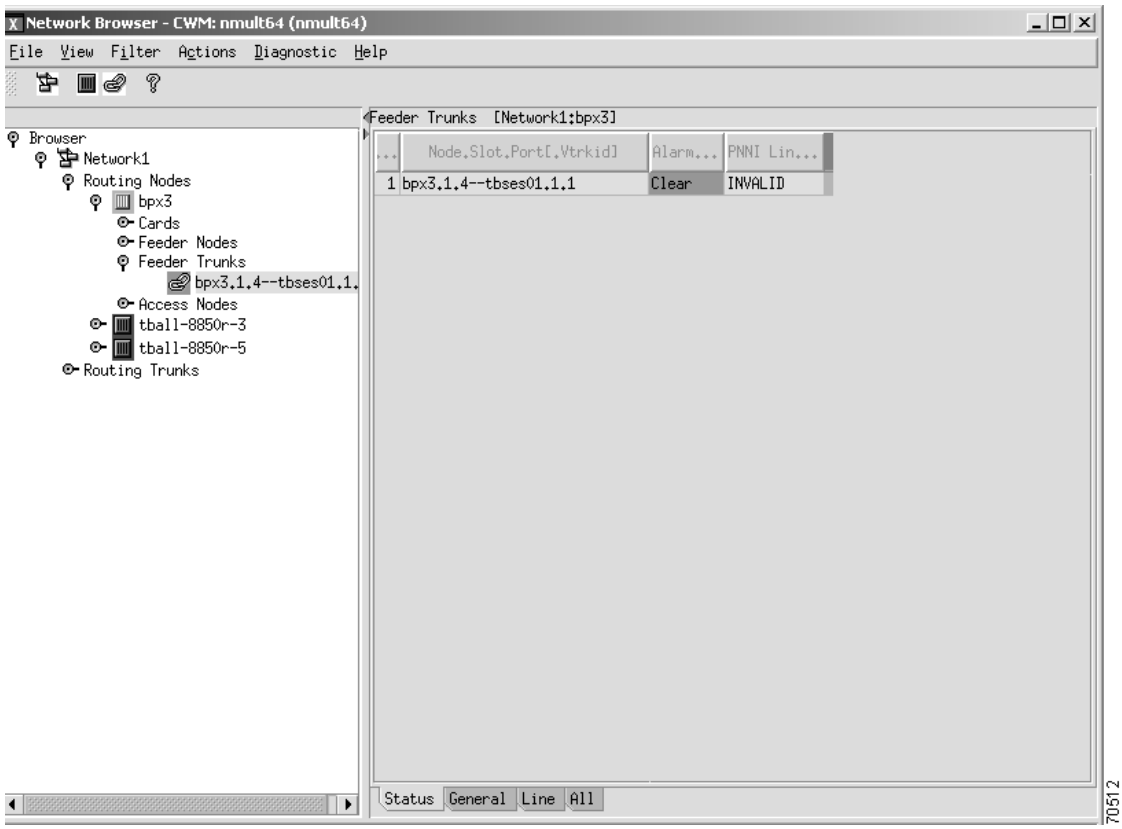


Figure 5-13 shows a selected feeder trunk in the left panel of the window, and its corresponding information in the right panel of the window.

Figure 5-13 Feeder Trunks

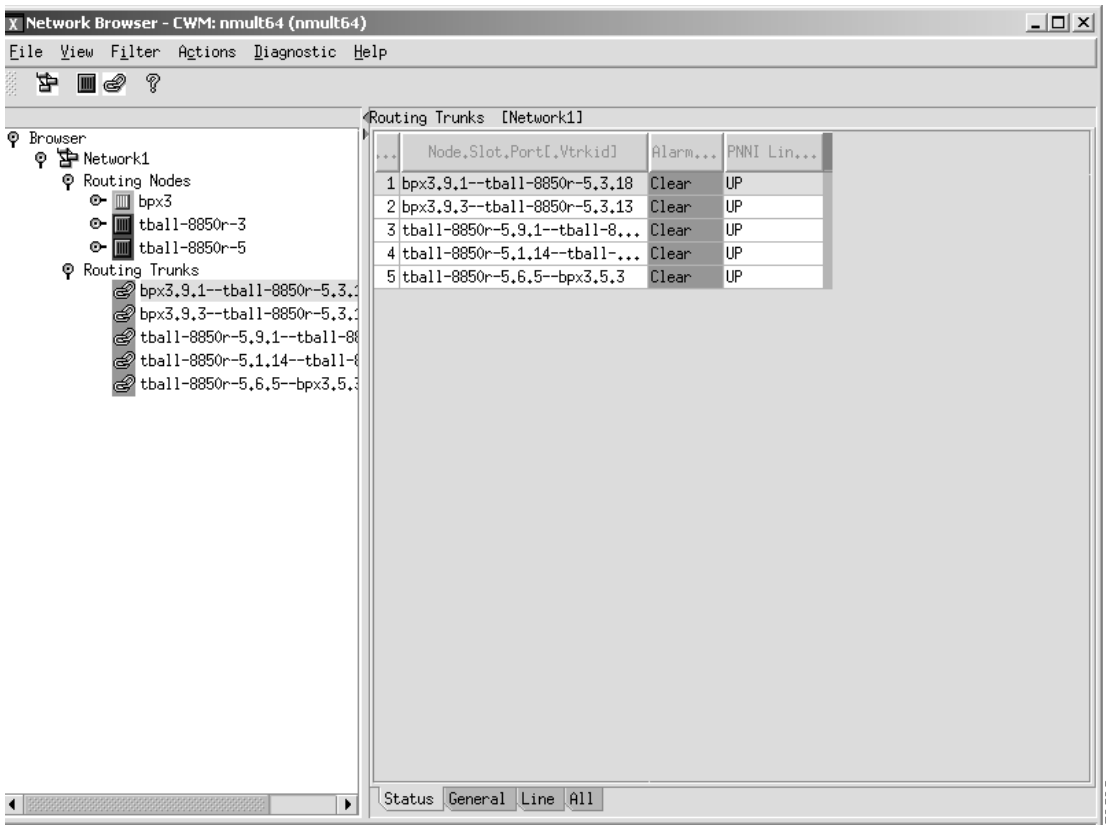


Click on the eye glass to the left of Access Nodes and its network elements will be displayed in the left panel of the window; select an element and the corresponding information will be displayed in the right panel of the window.

Routing Trunks

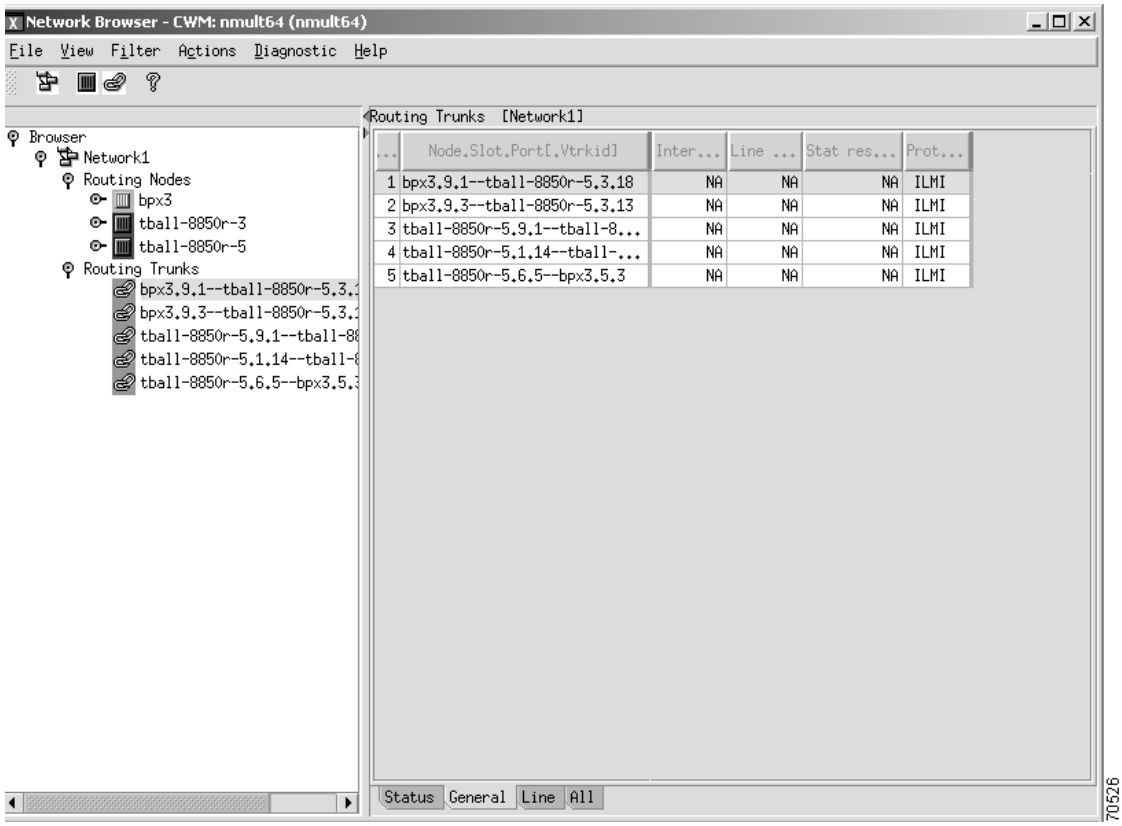
Click on the eye glass to the left of Routing Trunks to see the corresponding network elements. In Figure 5-14, bpx3.9.1 has been selected and the corresponding information appears in the right panel of the window. The default window for routing trunks is indicated by the **Status** tab located at the bottom of the Network Browser window and includes node.slot.port [vtrk.id] information, alarm status and PNNI link status.

Figure 5-14 Routing Trunks- Status Information



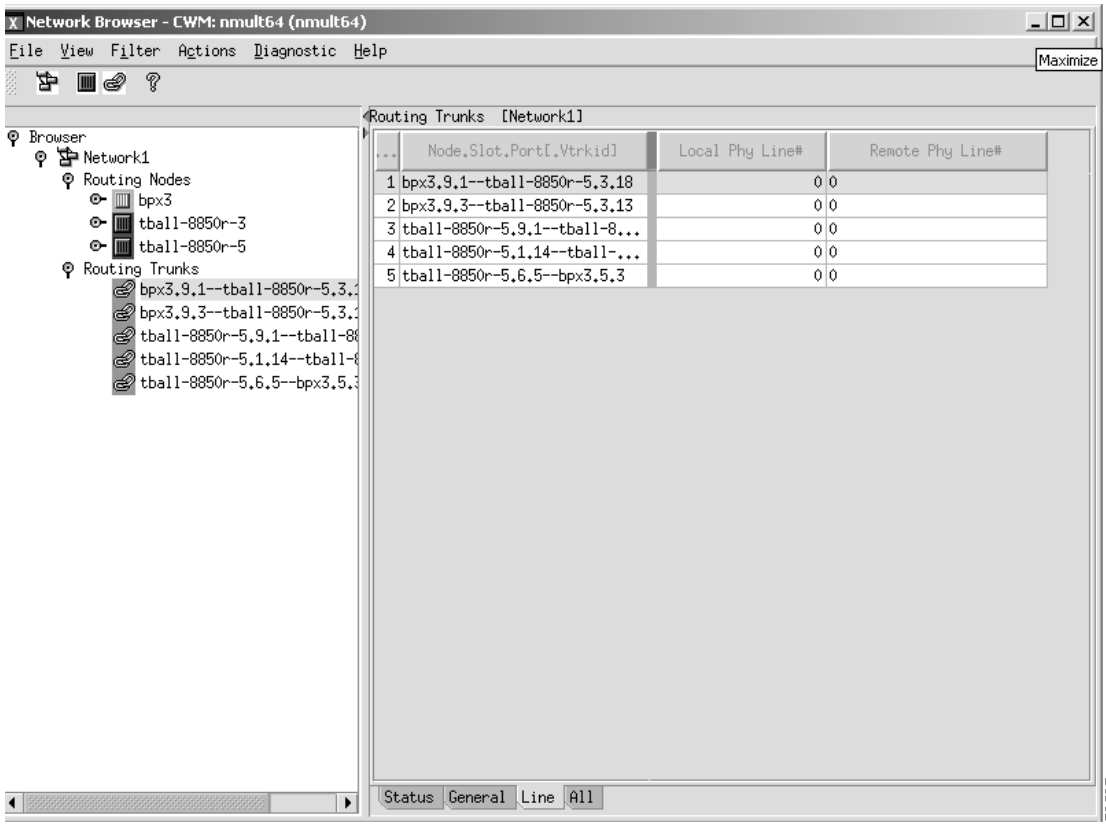
Click on the **General** tab to display additional information about the selected routing trunk including interface type, line load, statistical reserve and protocol information, as shown in Figure 5-15.

Figure 5-15 Routing Trunks- General Information



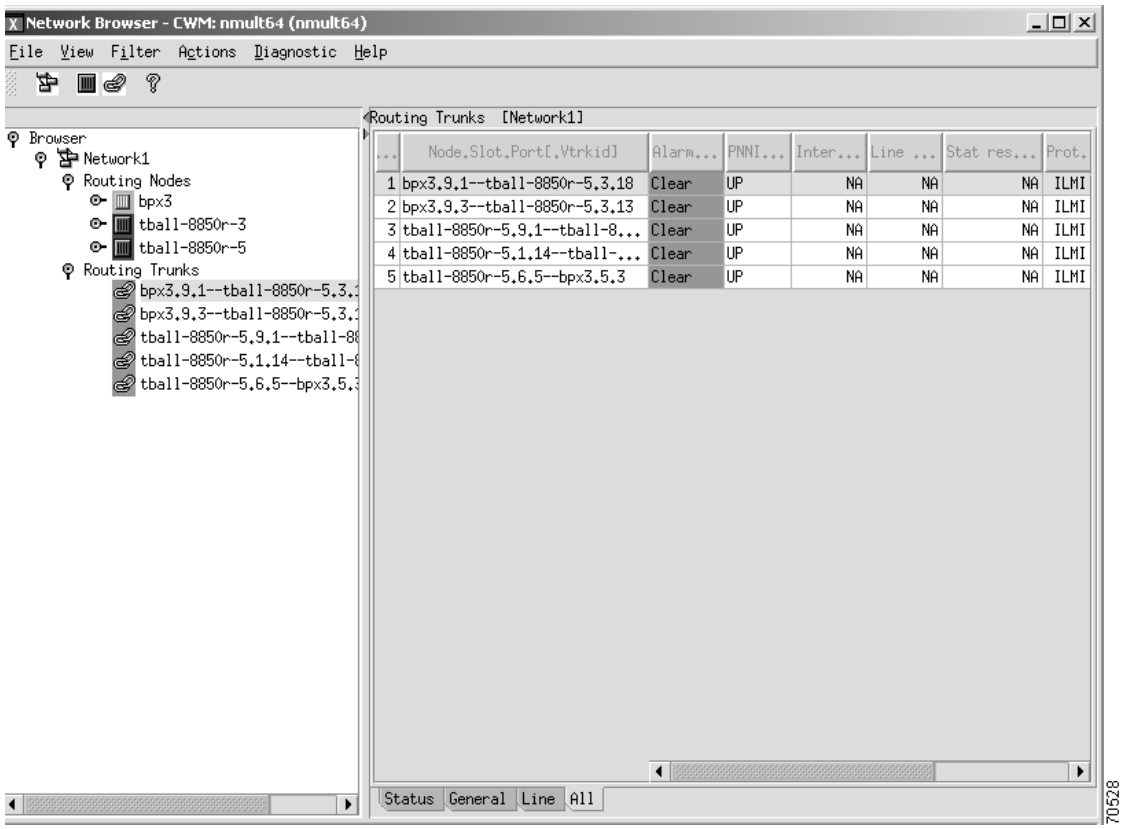
Click on the **Line** tab to display additional information about the selected routing trunk including local and remote physical line numbers, as shown in Figure 5-16.

Figure 5-16 Routing Trunks- Line Information



Click on the **All** tab to display additional information about all of these categories in one screen, as shown in Figure 5-17.

Figure 5-17 Routing Trunks- All Information Displayed



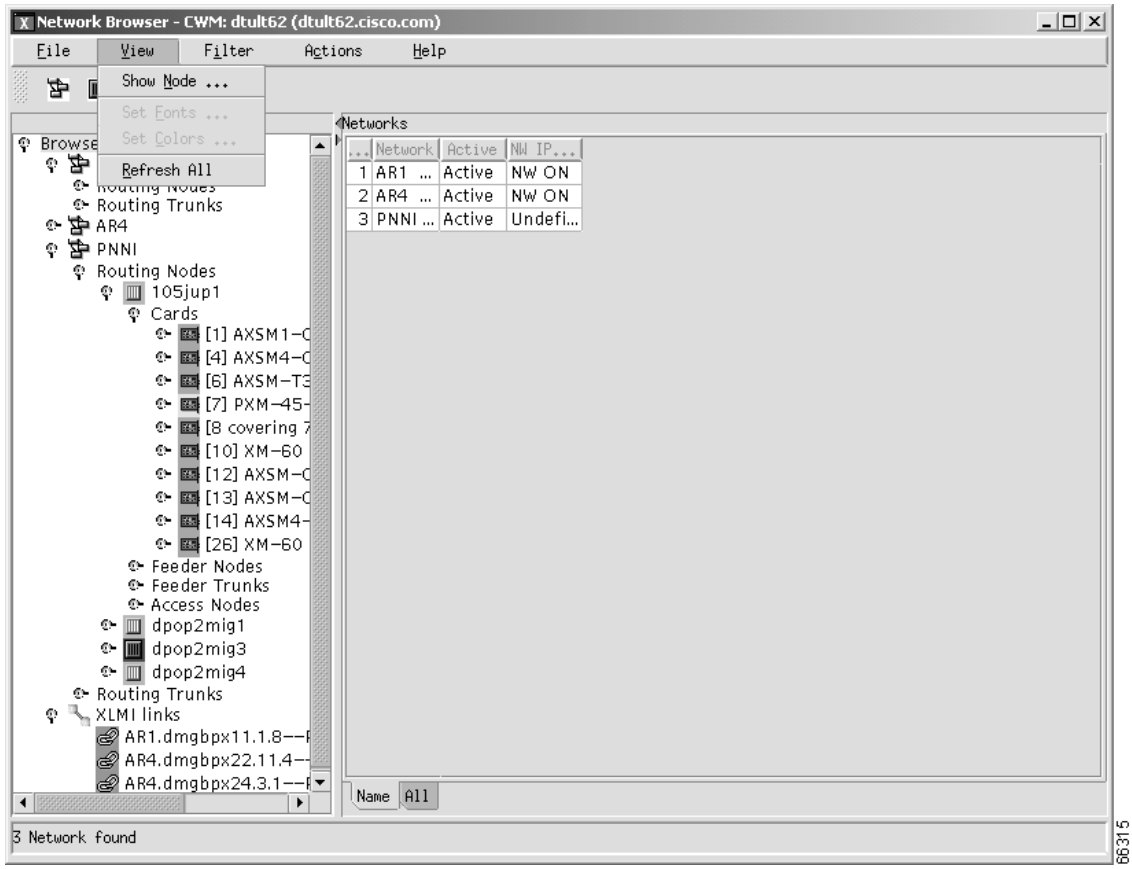
View Menu

The **View** menu, as shown in Figure 5-18, displays the **Show Node**, **Set Fonts, Set Colors,** and **Refresh All** submenus.

Select the **Show Node** option to view a node by name and a window will appear asking for the name of the node you want to view. Enter the node name and select OK. The node name will then be highlighted in the left panel of the window and the corresponding details of the node will appear in the right panel of the window.

Select **Set Fonts** or **Set Colors** to set how colors and fonts are displayed; the **Refresh All** option refreshes your current display.

Figure 5-18 View Menu



Filters

Using the Network Browser **Filter** menu, you can define filters for nodes or trunks by first selecting a node or trunk from the Routing Nodes or Routing Trunks display in the left panel of the Network Browser. Select the **Filter** pull down menu from the Network Browser main menu bar, and select either **Node** or **Trunk** to display filtering options. Only those resource(s) selected to filter are displayed in the Network Browser main window.

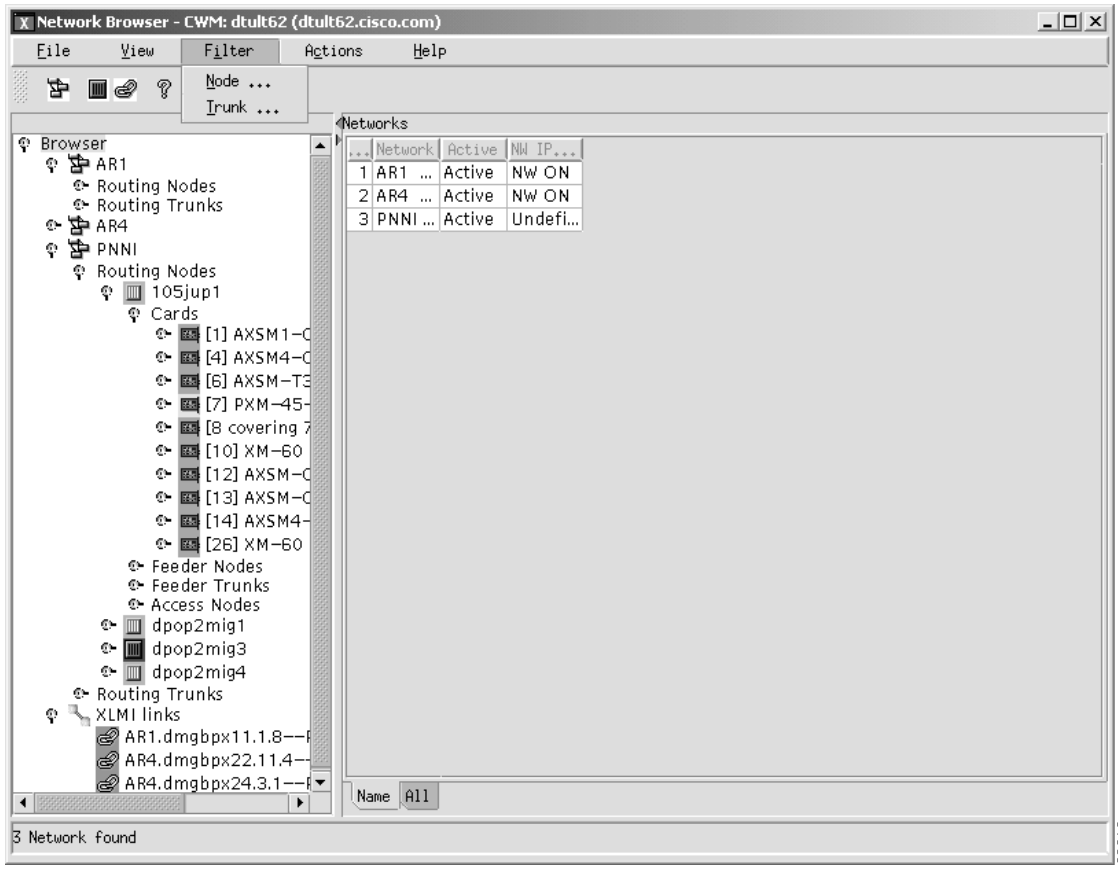
Filter Menu

The **Filter** menu, as shown in Figure 5-19, displays the **Node** and **Trunk** filter submenus. Select **Node** to filter by node name; select **Trunk** to filter by trunk name.

The **Node** option displays a window with a data field for the node name entry, and **Protocol**, **Type** and **Synchronized** tabs containing additional submenu options. The **Protocol** submenu allows you to select AR, TAG, PNNI, ILMI and/or Standalone options; the **Type** submenu allows you to select IGX, MGX, BPX and/or IPX switches; the **Synchronized** submenu asks you to select Yes or No for synchronization.

Additional node and trunk information is listed in Table 5-2, Node and Trunk Table Information.

Figure 5-19 Filter Menu



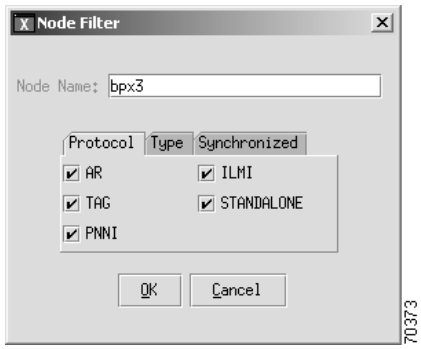
Node Filter

Node filtering can be defined for any node element in your network, from routing nodes and routing trunks, to individual card types, or node names beginning with a certain prefix. You can set up filters for all nodes or specify one of the following types:

- IGX 8400
- BPX 8600
- MGX 8850 (Stand-alone MGX 8850 nodes are displayed as a separate type)

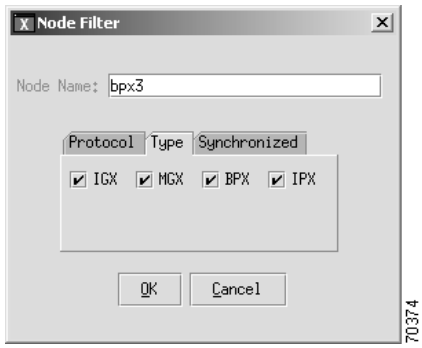
Node filtering can be defined for all node types with AutoRoute (AR), TAG, PNNI, ILMI and Standalone, or with all protocols, as shown in Figure 5-20.

Figure 5-20 Node Filter- Protocol



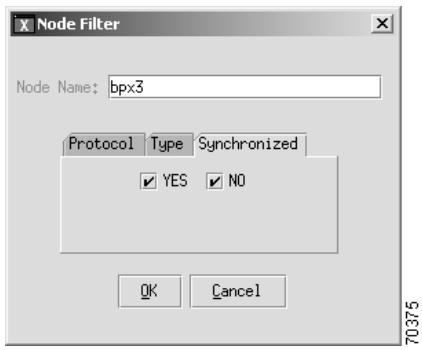
You can filter by type for all switches, all cards, certain cards, or certain interfaces, as shown in Figure 5-21.

Figure 5-21 Node Filter- Type



Node synchronization can be set to Yes, No, or both, as shown in Figure 5-22.

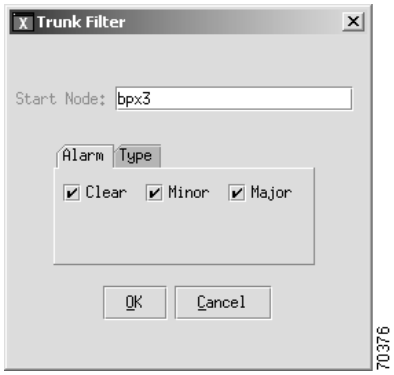
Figure 5-22 Node Filter- Synchronized



Trunk Filter

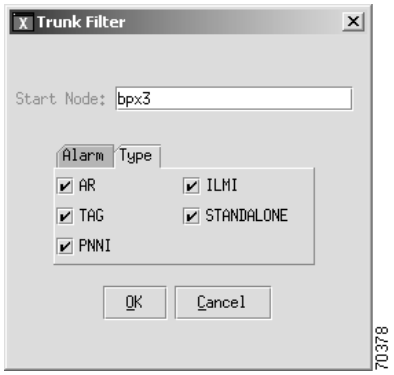
Figure 5-23 shows the trunk filter Alarm window with clear, minor and major alarm options.

Figure 5-23 Trunk Filter- Alarm



Trunk filtering can be defined for all trunk types, as shown in Figure 5-24, with AutoRoute (AR), TAG, PNNI, ILMI and Standalone options.

Figure 5-24 Trunk Filter- Type



Node and Trunk Tables

Table 5-2 Node and Trunk Table Information

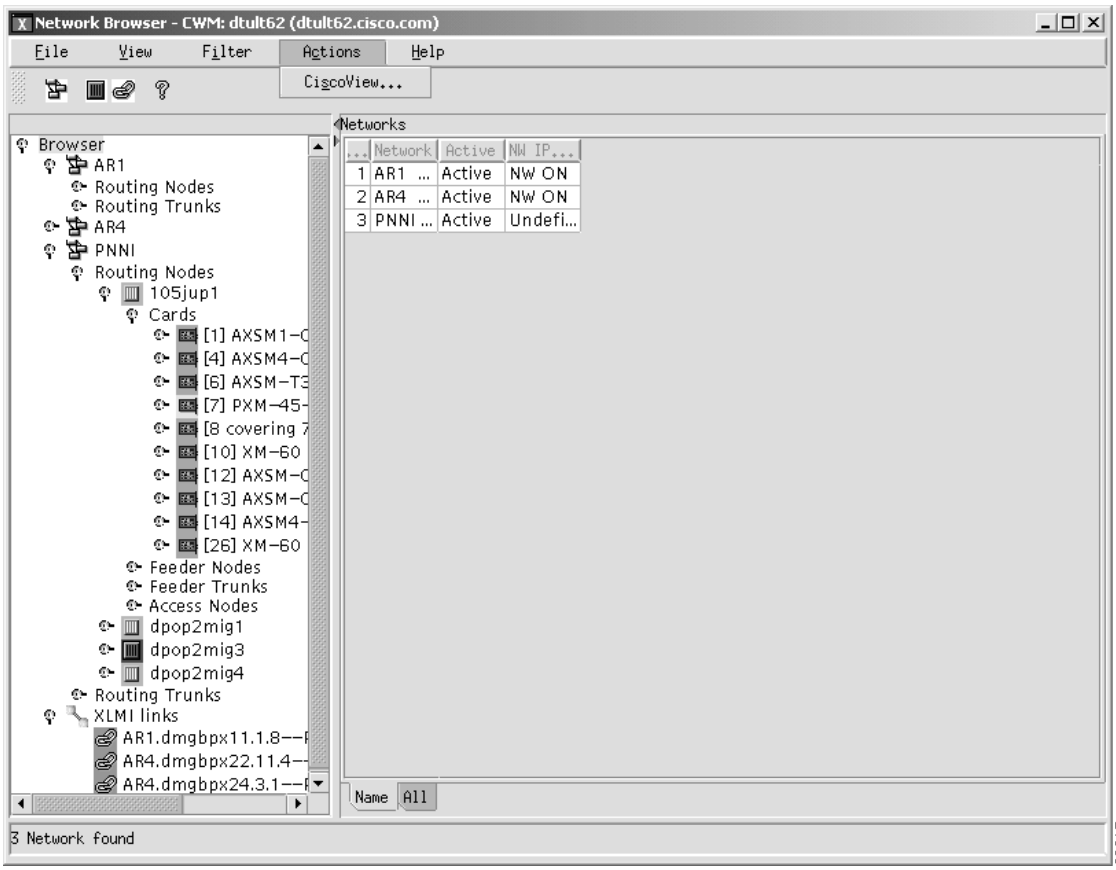
Node Column Headings	Meaning
Node Name	Name of the node
Alarm Status	Node alarm status shown in text and color: Normal (green) Minor (yellow) Major (orange) Critical (red) Unreachable (gray) Unknown (blue)
Management Status	Management status of the node (reachable or unreachable)
Synchronized	Yes/No synched. The node is synchronized if it's still synced up.
Revision	Switch software revision running on node
Network IP Address	Network IP Address
LAN IP Address	LAN IP Address (not applicable to all nodes)
Model/Type	Model string (if available) or type of node
Protocol	Protocols running on the node
Trunk Column Headings	**Meaning**
Name	Trunk Endpoints of format *name:slot:port*
Alarm Status	Trunk alarm status shown in text and color Normal (green) Minor (yellow) Major (orange) Critical (red) Unreachable (gray) Unknown (blue)
Interface	Trunk Interface
Line Load	Trunk Line Load
Stat Reserve	Statistics Parameter
Protocol	AR or PNNI

Note CWM uses color to display alarm situations detected by the Network Browser.

Actions Menu

The **Actions** menu, as shown in Figure 5-25, displays the **Cisco View** submenu. To view card, line and port configurations, select a card, line or port from the left panel of the Network Browser and then select the **Cisco View** submenu. The WAN Cisco View is a JAVA-based device management software GUI application that displays a graphical representation of the network device selected. Configuration and performance information is also presented on the selected card, line or port, and Cisco View will also perform minor configuration and troubleshooting tasks.

Figure 5-25 Actions Menu- Cisco View



XLMI

XLMI is a Cisco proprietary extension of the LMI protocol used to exchange IP addresses and to detect those connections associated with a XPVC segment. XLMI is a special kind of trunk designed to link AutoRoute Nodes and PNNI nodes. The following figures show XLMI links that are used in conjunction with the CWM Network Browser.

Figure 5-26 through Figure 5-29 show the status of a link, remote end of a connection, or both.

Figure 5-26 XLMI Links- Status

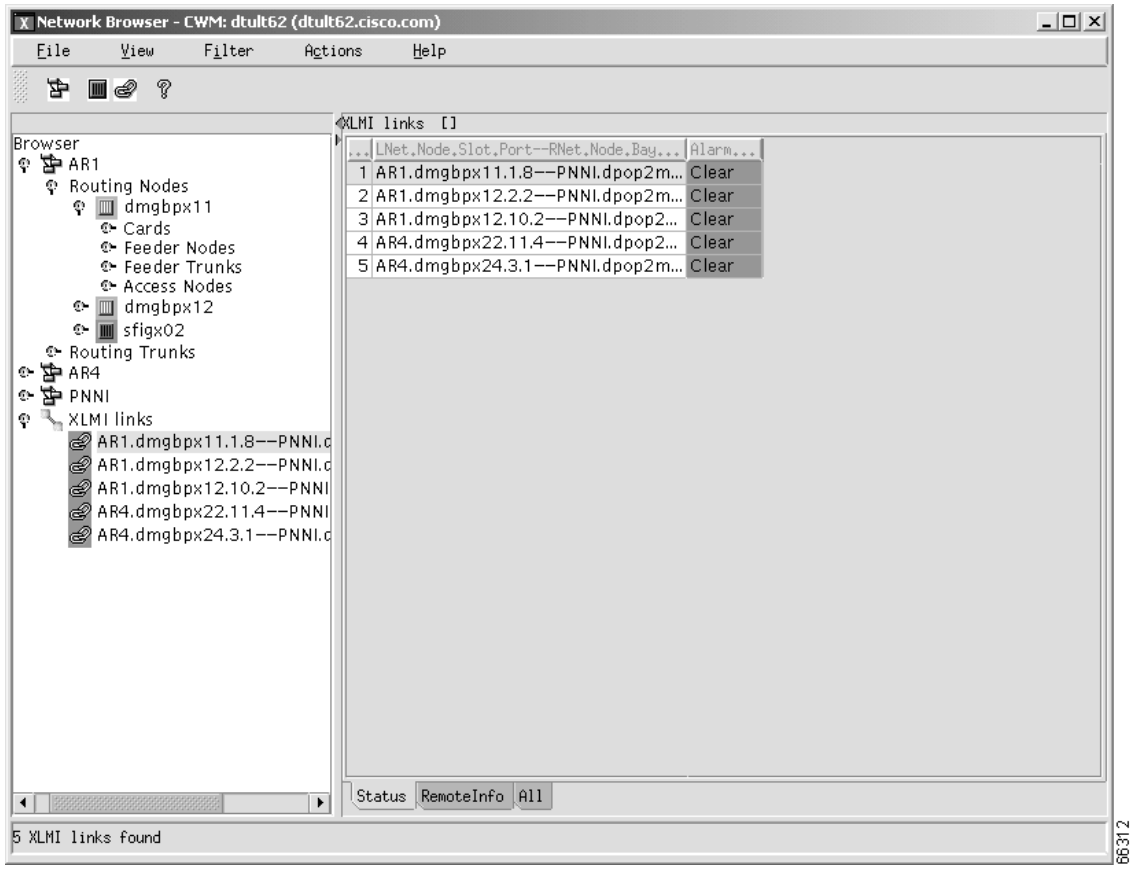


Figure 5-27 XLMI Links- Remote Information

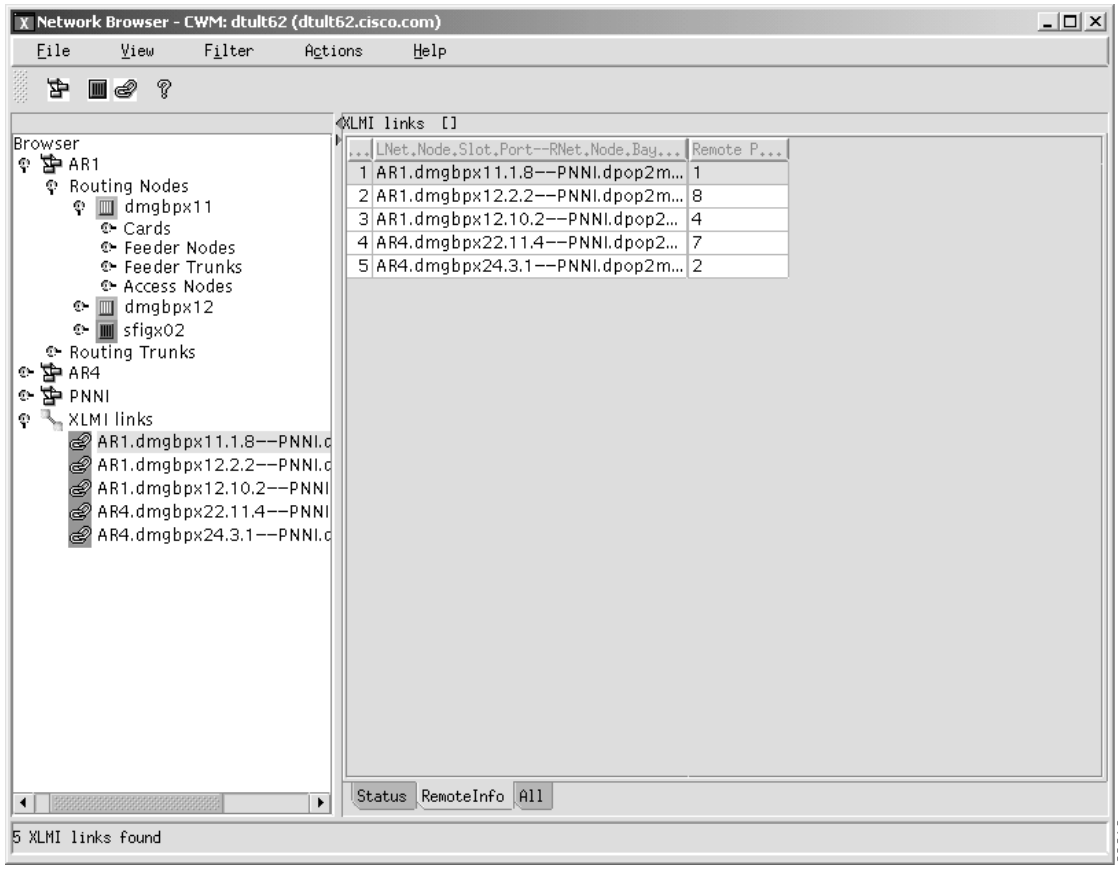


Figure 5-28 XLMI Links- All

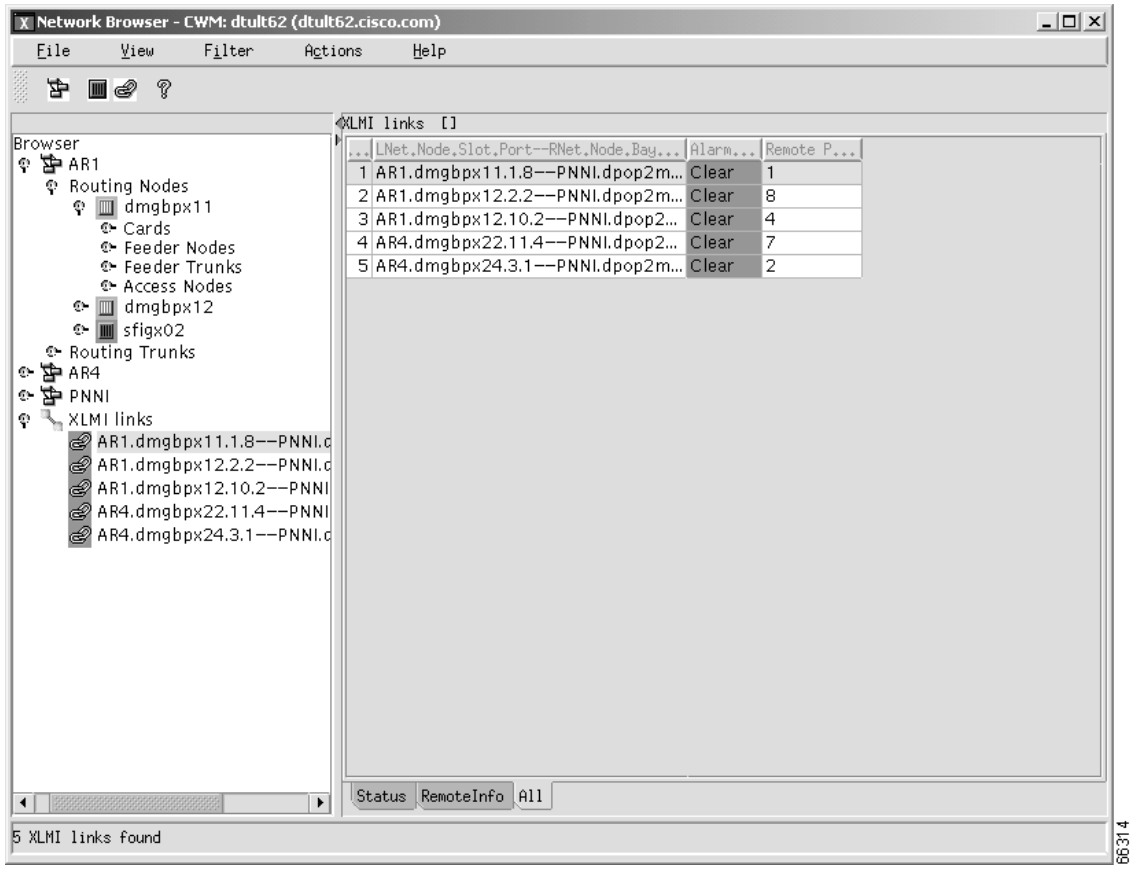
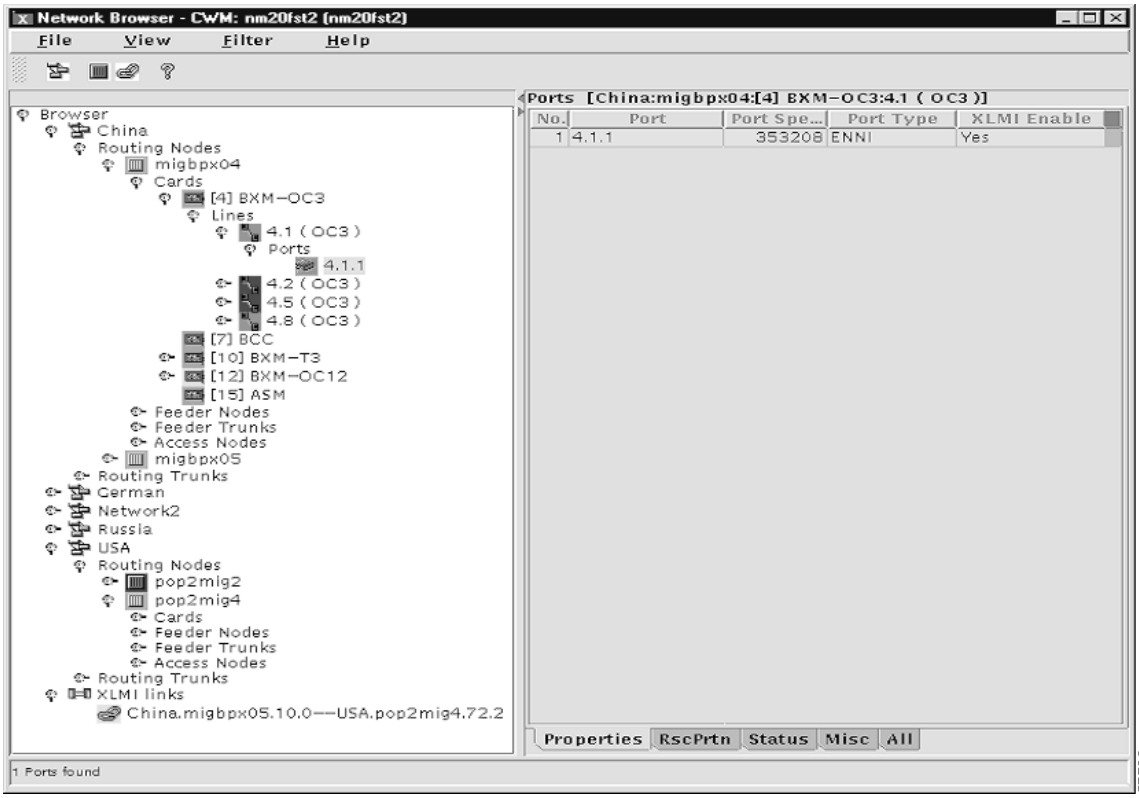


Figure 5-29 shows that XLMI is enabled. Notice that the farthest right columns of the ports display show an ENNI Port Type, and Yes below the column labeled XLMI Enable.

Figure 5-29 XLMI Enabled



Security Manager

Release 10 of CWM Security Manager (SM) is a new Java-based application that is launched from the desktop. The Security Manager provides controlled access to multiple users of Cisco WAN Manager (CWM), based on the user's UNIX User ID and password.

Security Manager provides user-access profiles that can be customized for each user. The user-access profile is a list of operations or actions a user can perform coupled with assigned access privileges for each action. A user can be assigned access privileges to read, create (write), modify, and/or delete.

By default, only the svplus user can start and stop the CWM core processes. The svplus user has sufficient access privileges to launch all CWM applications and administer the Security Manager application.

Other users can be assigned access privileges that enable them to perform operations within security-controlled applications. These operations can be limited depending on the setting of access privileges by those who administer Security Management. Without the proper access privileges, users cannot launch security-controlled applications.

Security Manager Requirements

To use CWM Security Manager application, you must first do two things:

- Use the **addnewuser** as root, to add a new Unix userID and password.

  Note Each CWM Security Manager user must have a unique Unix userID separate from their existing userID.

- The new user can be added to the CWM Security system by svplus (or any other security administrator), and access privileges assigned through the CWM Security Manager application.

To add a user, complete the following steps:

Step 1 At the CWM console prompt, enter su and provide a password.

```
host% su
```

Password:

Step 2 At the **root** prompt, enter the following:

./addnewuser <*username*>

where <*username*> is the name of the user to add.

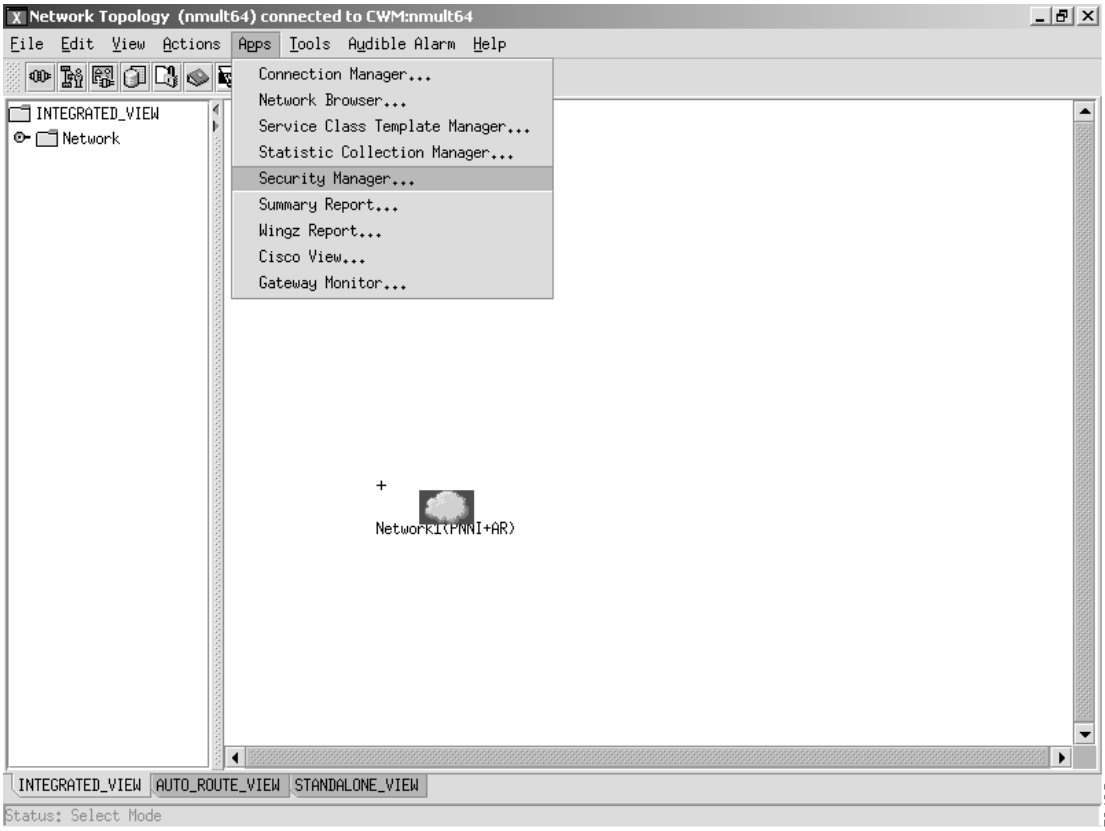
Note The # **./addnewuser <*username*>** command must be issued from the /usr/users/svplus/tools directory.

Step 3 Add the user to CWM using CWM Security Manager as described in Creating New Profiles, page 6-7.

Launching Security Manager

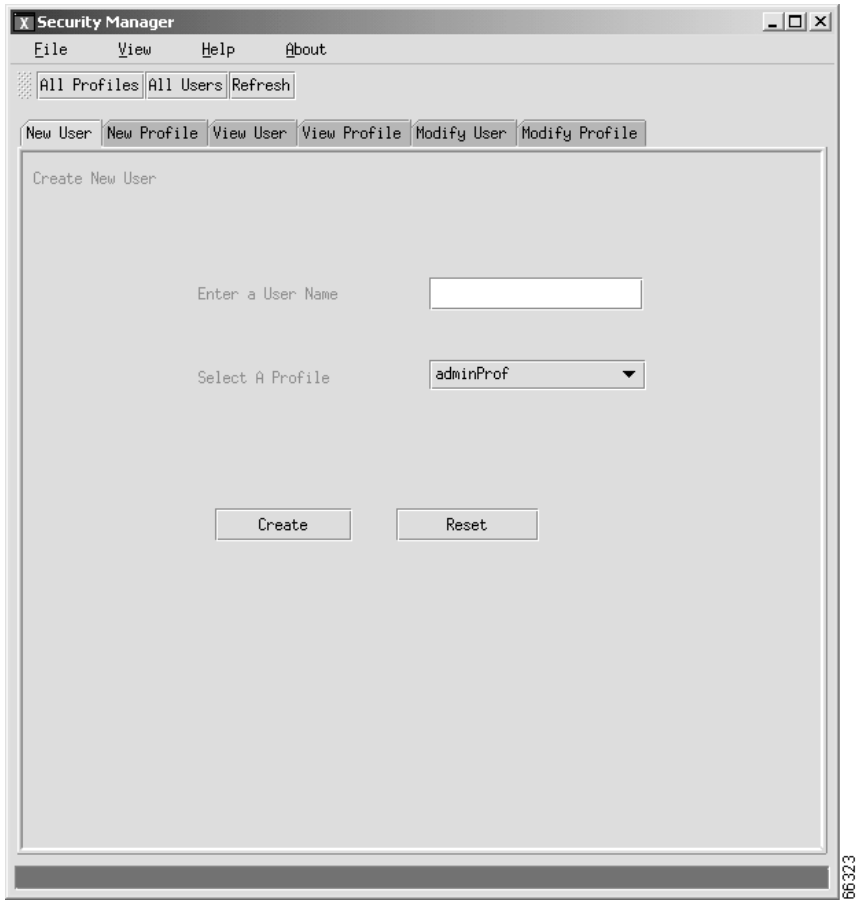
The Security Manager application is launched from the CWM desktop by clicking on the Security Manager icon, or by selecting **Security Manager** from the **Apps** pulldown on the menu bar of the CWM Topology main window, as shown in Figure 6-1.

Figure 6-1 Accessing Security Manager



After the Security Manager application is launched, the New User window is displayed by default as shown in Figure 6-2.

Figure 6-2 New User window



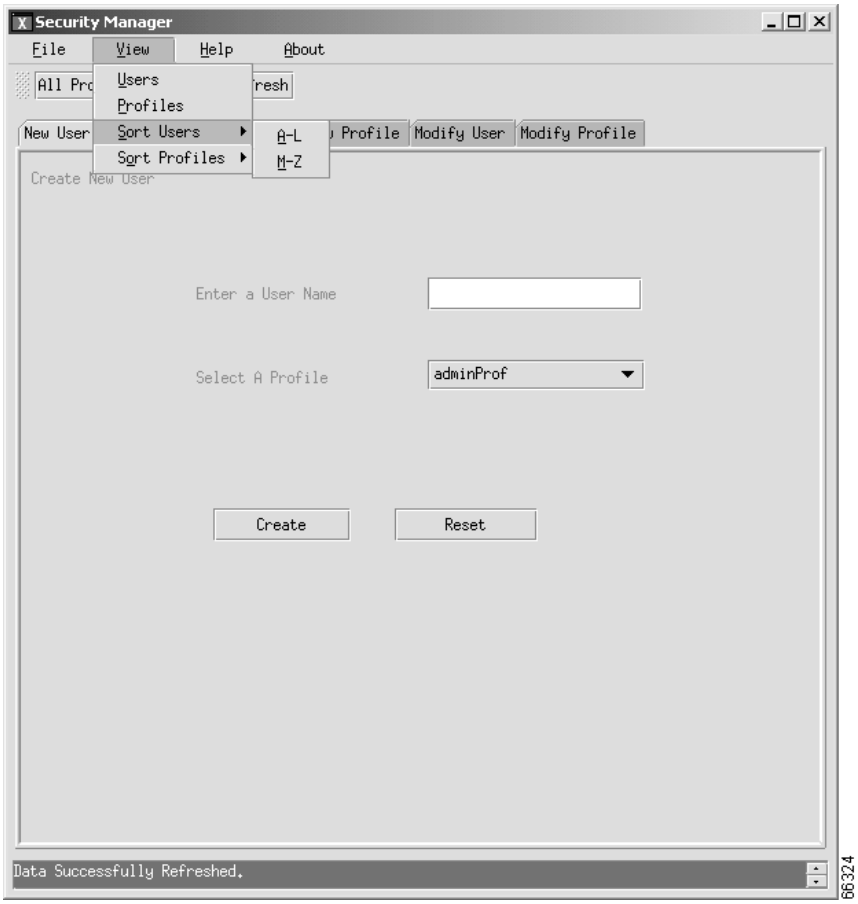
Menu Options

The Security Manager application has four menu options: **File**, **View, Help and About**. Under the **File** menu you will find the **New** menu, with **User** and **Profile** submenus. The **User** submenu takes you to the Create New User tab; the **Profile** submenu takes you to the Create New Profile tab.

The **Exit** menu is the second menu option available under the **File** pulldown. When you select **Exit**, a confirmation dialog box is displayed, giving you an opportunity to save the configuration with any unsaved changes.

Four options are provided under the **View** menu, as shown in Figure 6-3,: **Users**, **Profiles, Sort Users** and **Sort Profiles**. Selecting **Users** takes you to the View User window; selecting **Profiles** takes you to the View Profile window. The **Sort Users** and **Sort Profiles** submenus bring up dialog boxes with users or profiles sorted from **A-L** or **M-Z**.

Figure 6-3 The View Menu Option

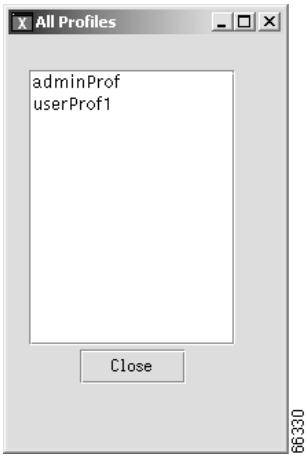


The **Help** menu helps you to select the appropriate privileges for a profile; the **About** menu shows you the CWM Security Manager version release.

Button Options

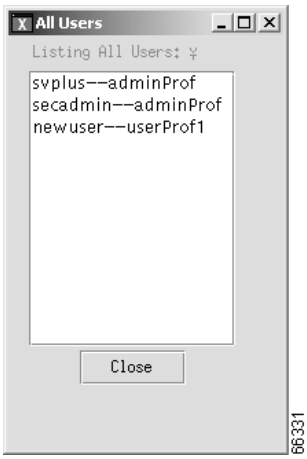
The Security Manager main menu bar also provides the **All Profiles** button which displays the **All Profiles** window, as shown in Figure 6-4, and the **All Users** button displays the **All Users** window, listing those users who have Security Manager Admin privileges, as shown in Figure 6-5. The **Refresh** button refreshes user data, as shown in Figure 6-6.

Figure 6-4 All Profiles window



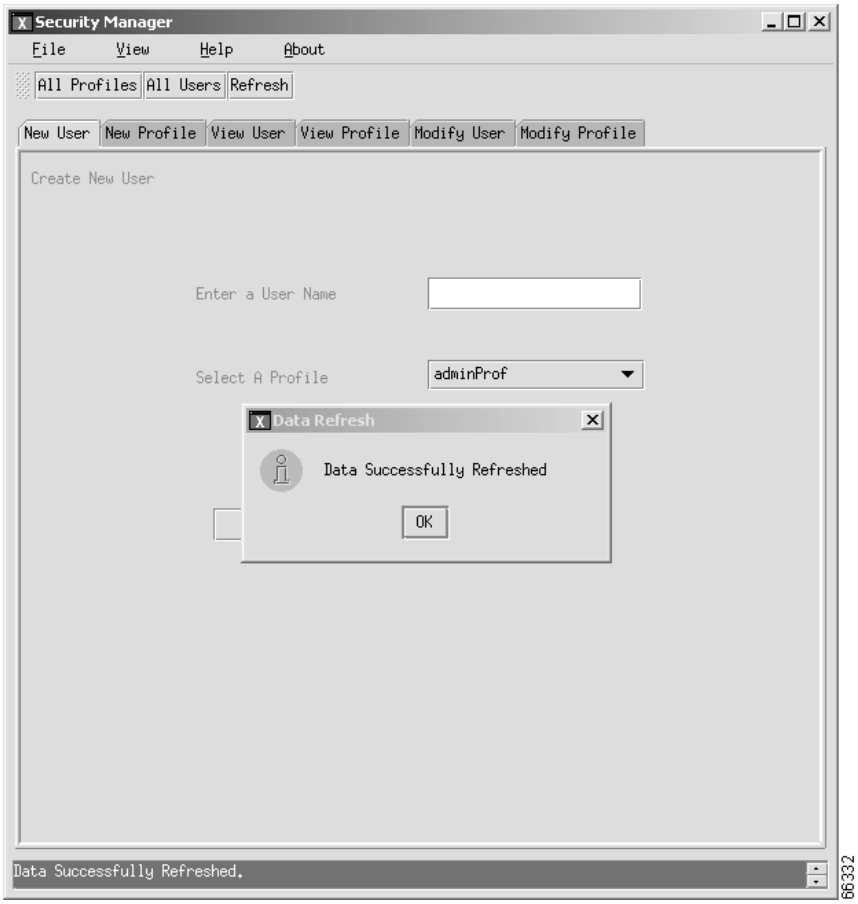
Note When you install CWM software, two default access profiles are created: adminProf and userProf1.

Figure 6-5 All Users window



Note When you install CWM software, three default users are created: svplus, secadmin, newuser.

Figure 6-6 Refresh window



New User

To create a new user, complete the following steps:

Step 1 From the Security Manager window, select the **New User** tab as shown in Figure 6-2.

Step 2 **Select a profile from the drop-down combo box**.

Step 3 Click the **Create** button to create a new user.

Note Only those users who have **Create** or **All** permissions can create new users.

Creating New Profiles

You can create profiles to allow users to perform specific tasks within CWM. For example, you can create a profile to give a user read privilege for Network Topology or create and modify privileges for Connection Manager.

You create profiles through the **New Profile** window of the Security Manager main window. When the **New Profile** window is first displayed, as shown in Figure 6-7, boxes that are shown in **bold** typeface are the only ones that can be selected.

Access Privileges

Security Management is provided at the application level. Users are granted access to controlled applications depending on their access privileges.

Using the **New Profile** window, you can create a security profile to give a user read, create, modify, or delete privileges to one or more of the controlled applications. You can set up a profile to grant all privileges to one of the applications and some privileges to another application. You can create a profile for users who only require read access to enable them to observe an application's windows, and at the same time provide detailed security control. Detailed information about which functions are available is presented with the applications.

The functionality for access privileges depends on the application. Privileges are mapped to different functions in different applications.

Table 6-1 lists the access privileges for CWM applications.

Table 6-1 Applications and Access Privileges

Function	Read	Create	Modify	Delete	All
Connection Manager Connections					X
Statistics Collection Manager					X
Configuration Save & Restore					X
Network Topology					X
Service Class Template Manager					X
Wingz	X				
CWM Admin	X				
Network Browser	X				
Summary Reports	X				
Security Manager Admin					X
Cisco View	X				
Image Download		X			
Node Resync	X				
spvcPreferred Configurator					X

Note Unless Network Topology has Read permissions, Config Save & Restore, Image Download, and Node Resync cannot be selected. Also, if any of these three applications are selected in a profile, Network Topology cannot be de-selected.

Read Privileges

With read privileges a user can view displays and topology windows, list connections, and other functions where information is read. Read privileges are similar to the svplus-r account from earlier releases of CWM.

Create Privileges

With create privileges, a user can create and configure connections, perform association backup, and add nodes, ports, and trunks.

Modify Privileges

With modify privileges, a user is also granted read privileges. A user with modify access can modify connections, ports, and trunks, and add and delete nodes and groups.

Delete Privileges

With delete privileges, a user is also granted read privileges. A user with delete access can delete connections, ports, trunks, nodes and groups.

All Privileges

If granted all privileges, a user has read, create, modify and delete privileges for the associated application.

New Profile

To create a new security profile, complete the following steps:

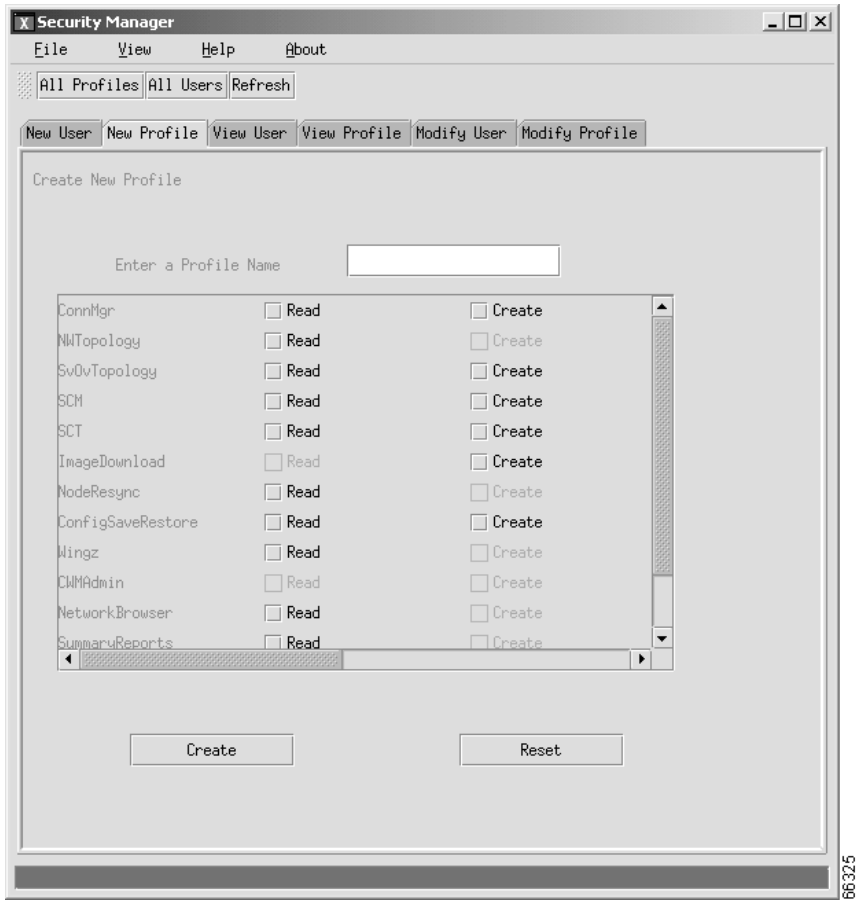
Note Only users who have **Create** or **All** privileges for Security Manager can create a new profile.

Step 1 From the Security Manager window, select the **New Profile** tab as shown in Figure 6-7.

Step 2 **Enter a Profile Name** in the data field.

Step 3 Select all desired access privileges and then click **Create** to create the new profile.

Figure 6-7 New Profile window



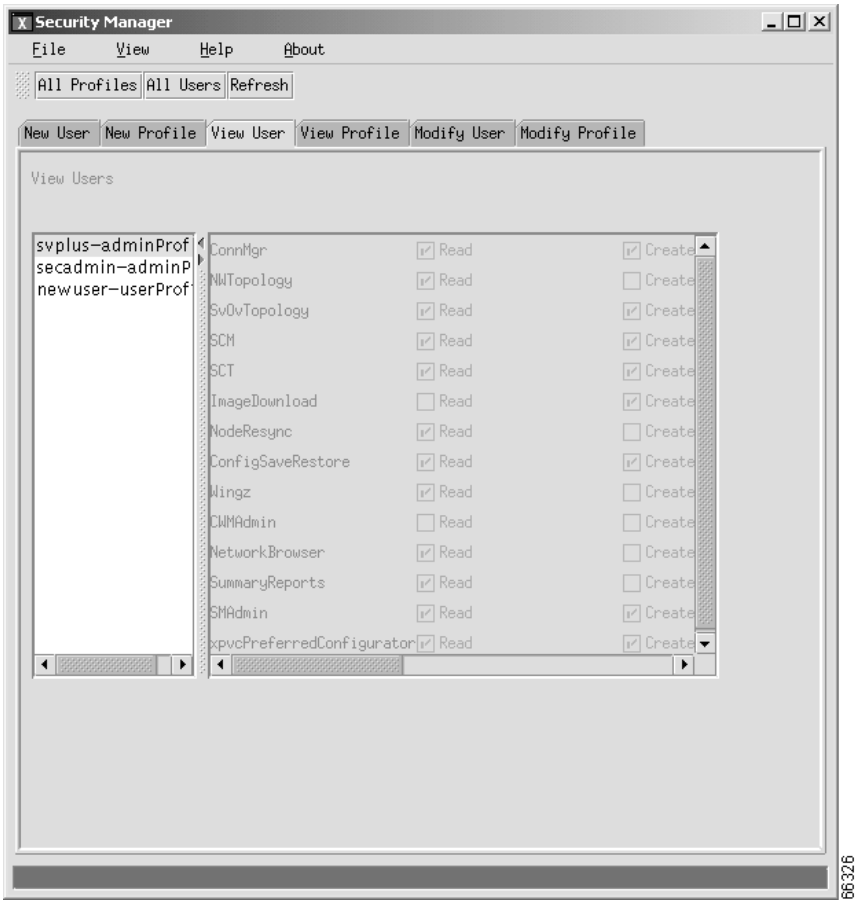
View User

To view a user, complete the following steps:

Step 1 From the Security Manager window, select the **View User** tab as shown in Figure 6-8.

Step 2 Select the user you want to view from the list of users in the left panel of the window. The access privileges for the selected user will be listed in the right panel of the window. All applications and their access privileges are grayed out. Unchecked boxes indicate the absence of a particular privilege in a specific application.

Figure 6-8 View User window



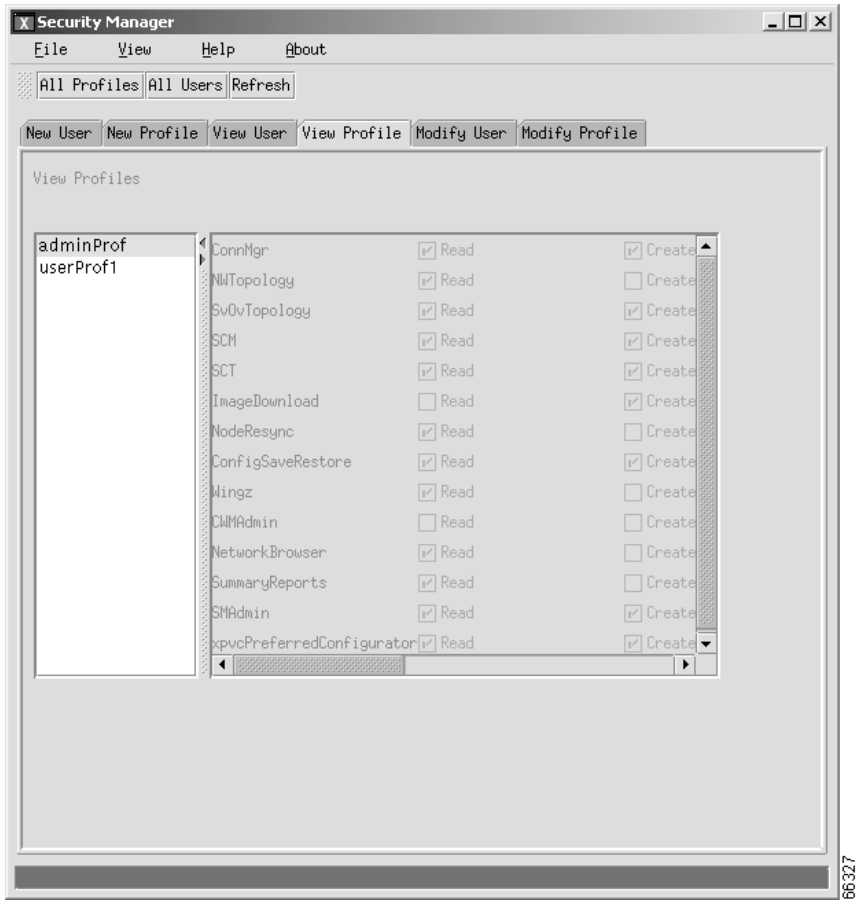
View Profile

To view a profile, complete the following steps:

Step 1 From the Security Manager window, select the **View Profile** tab as shown in Figure 6-9.

Step 2 Select the profile you want to view from the list of profiles in the left panel of the window. The access privileges for the selected profile will be listed in the right panel of the window. All applications and their access privileges are grayed out. Unchecked boxes indicate the absence of a particular privilege in a specific application.

Figure 6-9 View Profile Window



Modifying Users

To modify a user, complete the following steps:

Step 1 From the Security Manager window, select the **Modify User** tab as shown in Figure 6-10.

Step 2 Select the user to modify by selecting the appropriate **User Name-Current Profile**.

Step 3 **Select New Profile** for the user, and then click **Save**.

Deleting Users

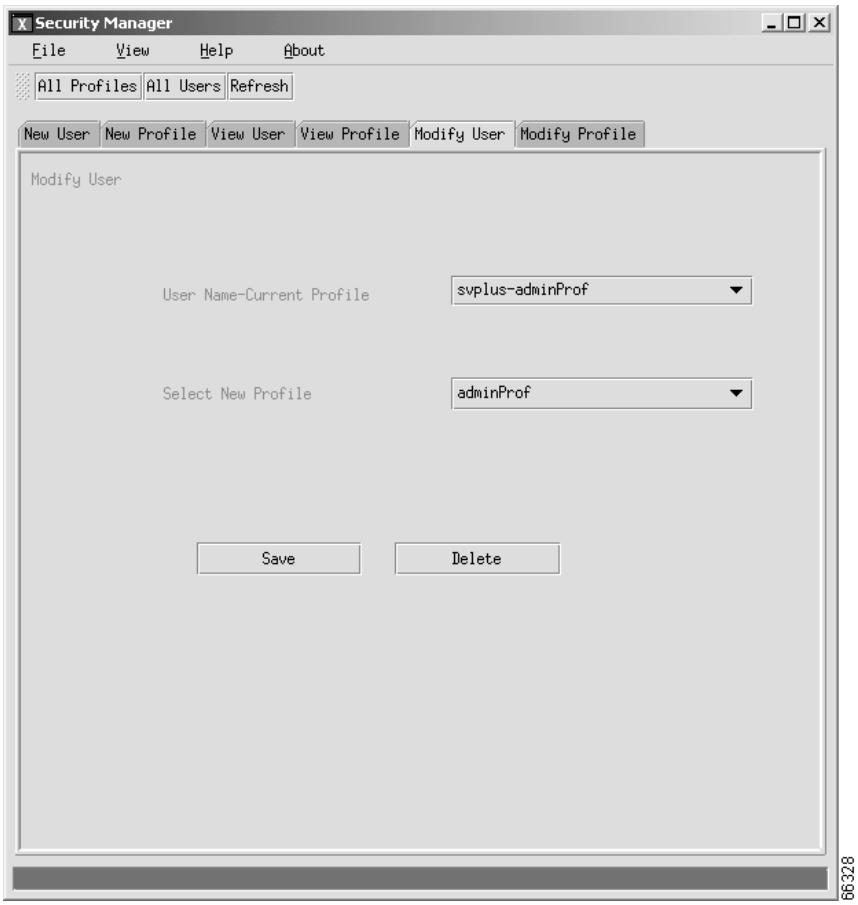
To delete a user, complete the following steps:

Step 1 From the Security Manager window, select the **Modify User** tab as shown in Figure 6-10.

Step 2 Select the user to delete by selecting the appropriate **User Name-Current Profile**, and then click **Delete**.

Step 3 On the confirmation dialog, click **Yes** to delete the selected profile.

Figure 6-10 Modify User window



Modifying Profiles

After a profile has been created, you can easily modify it. To modify an existing profile, complete the following steps:

Step 1 From the Security Manager window, select the **Modify Profile** tab as shown in Figure 6-11.

Step 2 Select the profile to modify by clicking on the profile name.

Step 3 Select access privileges for the profile you want to modify from the **Read**, **Create**, **Modify**, **Delete** and **All** privilege options, which are displayed in the right panel of the **Modify Profile** window.

Step 4 Click **Save** to save modifications to the selected profile.

Step 5 Click the **Users with Profile** button to list users with the modified profile.

Deleting Profiles

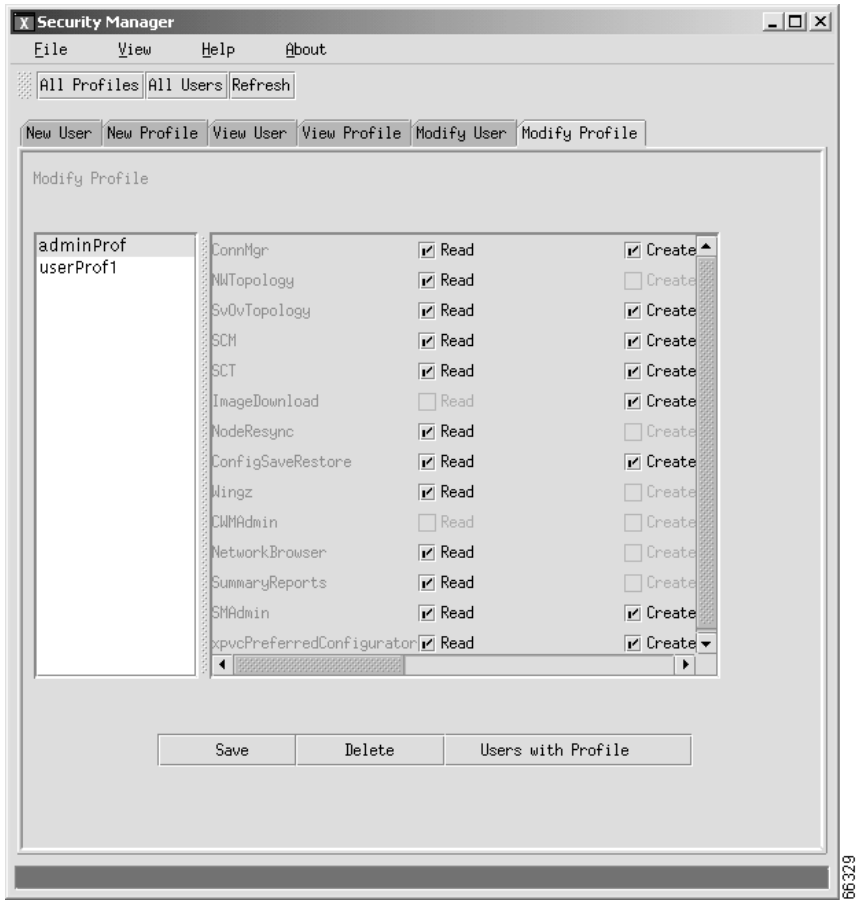
To delete a profile, complete the following steps:

Step 1 From the Security Manager window, select the **Modify Profile** tab as shown in Figure 6-11.

Step 2 Select the profile to delete by clicking on the profile name, and then click **Delete**.

Step 3 On the confirmation dialog, click **Yes** to delete the selected profile.

Figure 6-11 Modify Profile window



Controlled Applications

Security Manager is supported on CWM applications launched from the CWM desktop, from HP OpenView, and from the UNIX command line prompt. The following tables list the CWM applications and their supported access privileges. An “X” within an access privilege column indicates that the privilege applies to the operation. If the column is blank, the access privilege does not apply to the operation.

Table 6-2 lists the access privileges required for applications launched from the CWM desktop

Table 6-2 Desktop Application Security Matrix

Desktop Application	Read	Create	Modify	Delete	All
Network Topology	X				
Image Download		X			
Config Save & Restore	X				
Security Manager	X				
Wingz	X				
Connection Manager GUI	X				
Network Browser	X				
CWM Administrator					
Summary Reports	X				
xpvc Preferred Configurator	X				

Table 6-3 lists the access privileges required for applications launched from the HP OpenView.

Table 6-3 HP OpenView Applications Security Matrix

HPOV Applications	Read	Create	Modify	Delete	All
SVOV Topology					
Event Log					
Image Download					X
Node Resync					X
Configuration Save					X
Configuration Restore					X

Table 6-4 lists the access privileges required for applications launched from the UNIX prompt.

Table 6-4 UNIX Prompt Applications Security Matrix

UNIX Prompt Applications	Read	Create	Modify	Delete	All
Statistics Collection Manager					X
Cisco View Lines/Trunks					X
Connection Proxy					
Port Proxy					

Connection Manager

Table 6-5 lists the access privileges required to perform security-controlled operations within the Connections Manager application.

Table 6-5 Connection Manager Access Privileges

Access Privilege	Connection Manager Operations
Read	Able to list connections and view multicast connections and templates
Create	Able to configure connections and perform association backup
Modify	Able to modify connections; also able to list connections, view multicast connections and templates (read access privileges)
Delete	Able to delete connections; also able to list connections and view multicast connections and templates (read access privileges)

Network Topology

The CWM Network Topology application is linked to Security Manager which checks a user's access privileges before providing access to the Topology application on the CWM desktop. A user without access privileges will find the Topology icon on the CWM desktop to be grey, inactive, and unable to launch the Topology application. Table 6-6 lists the access privileges.

Table 6-6 Topology Access Privileges

Access Privilege	Topology Operations
Read	Able to view topology windows.
Create	Able to add nodes and view topology windows (read access privileges).
Modify	Able to make modifications to topology maps.
Delete	Able to delete nodes, delete groups, and view topology windows (read access privileges).

Statistics Collection Manager

The CWM Statistics Collection Manager is linked to Security Manager which checks a user's access privileges before providing access to SCM. A user without access privileges will not be able to launch the SCM application.

Table 6-7 lists the access privileges required to perform security-controlled operations within the SCM application.

Table 6-7 SCM Access Privileges

Access Privilege	SCM Operation
Read	Enables Show Collection Information option
Create	Enables Stats Enable option
Modify	Enables Start Collection option
Delete	Enables Stop Collection option

Service Class Template Manager

This chapter describes the CWM Service Class Template (SCT) desktop application. The SCT application allows users to map standard connection protocol parameters for AXSM, AXSM-E, and RPM cards using a set of data structures that associate VSI service types to sets of pre-configured Virtual Channel (VC), and Class of Service Buffer (CoSB) parameters.

SCT Overview

The Service Class Template application is a Java based CWM process that allows for creating SCT files which can then be loaded to nodes, and can be associated with interfaces on cards within the nodes. This application is launched from the CWM desktop and allows users and network operators to configure AXSM, AXSM-E, and RPM cards, using the Service Class Template feature. Specifically, users or network operators are able to use the SCT application to create, modify, delete, download, and associate SCT files to AXSM cards and ports.

VC Descriptor

The Virtual Channel Descriptor Template is a component of a Service Class Template that contains platform specific VC configuration, and is indexed primarily by Service Type. A Service Type is a concept for grouping connections that share a common set of traffic characteristics and QoS (Quality of Service) requirements. The VC Descriptor Template defines SCT parameters that are applied to all VCs and that match a specified Service Type. As defined in the SCT MIB for the AXSM card, a VC Descriptor for AXSM consists of 36 elements, including the SCT ID, of which the VC Descriptor is a part, the Service Type and the CoSB (Class of Service Buffer) number, which indicates the CoSB used for the connections.

CoSB Descriptor

The Class of Service Buffer is a buffer or queue that serves connections with similar QoS requirements. A CoSB Descriptor Template contains CoSB configurations, with 18 attributes for AXSM cards indexed by CoSB number.

SCT Load

The sctLoad utility included in CWM Release 10.5 is a tool designed for uploading SCT files that will be used for provisioning. There are a number of pre-configured default files available, including SCT2, SCT3, SCT4, and SCT5.

Note SCT2 and SCT3 are used for PNNI, and SCT4 and SCT5 are used for MPLS; SCT2 and SCT4 are used for policing, and SCT 3 and SCT 5 are used for no policing.

The following output informs the user that there are additional parameters which are not used for SCT2 and SCT3. This informative output appears when using sctLoad to load SCTs versions 2.0 and earlier into a system which operates on SCTs for PXM 45, Release 2.1. The SCTs for PXM 45, Release 2.1 contain MPLS data which is not present in the earlier versions of SCTs. In this case, the sctLoad utility informs the user that this data is missing and that it is inserting default data into the missing fields in order to upgrade the SCT files to the latest SCT format. When SCT2 or SCT3 are uploaded, the sctLoad utility will add default values to the missing fields, as shown in the example:

```
sjnms12% sctLoad -f AXSM_SCT.PORT.5
SCT VC data (12, 6) undefined, setting to default (1)
Exiting SctLoad ...

sjnms12% sctLoad -f AXSM_SCT.CARD.2
SCT VC data either undefined or missing due to old file format.
 Setting missing data to default values...
Exiting SctLoad ...
```

Note The sctLoad utility has successfully finished loading SCT file(s) when "Exiting SctLoad ... " appears at the bottom of the output screen.

Note It is recommended that the user hits the Enter key after modifying any parameter values within an SCT file.

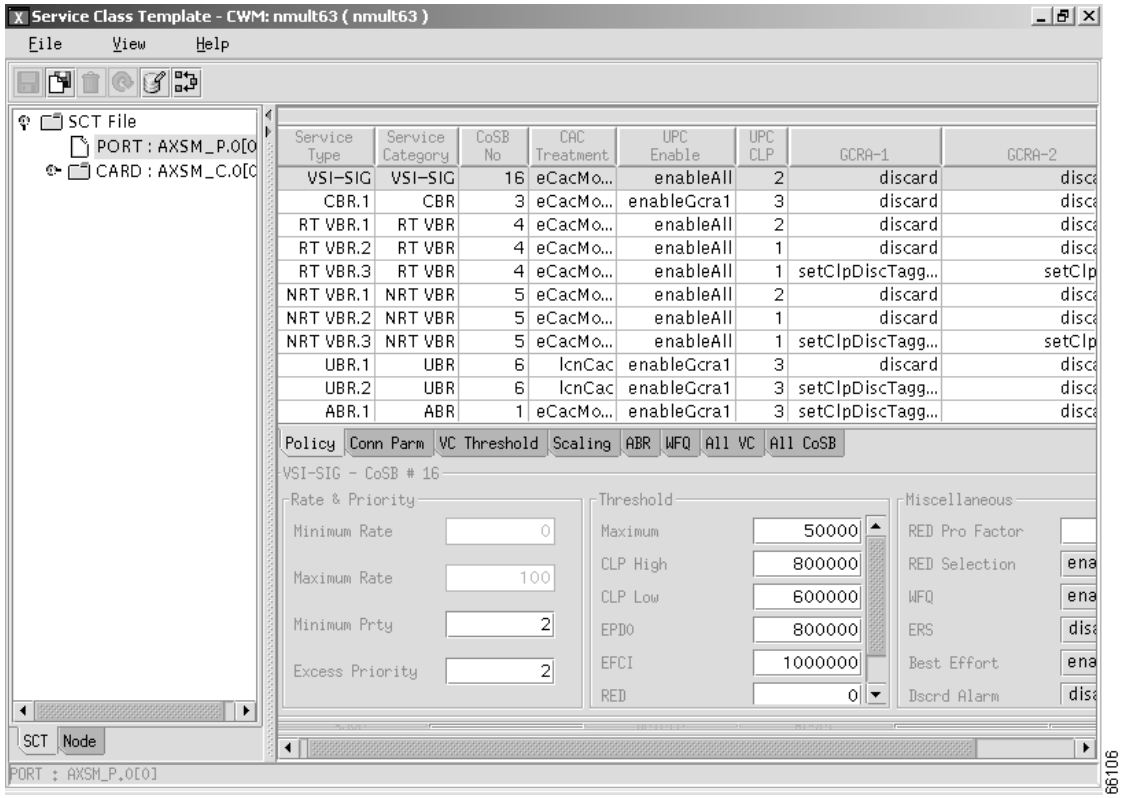
Initializing SCT

When a PXM card is installed for the first time it does not have SCT files. Therefore, the user must upload SCT 2, 3, 4 and 5 files from the switch to CWM via the sctLoad utility. The user will first need to FTP the files from the switch to the directory `~svplus/sct-file/1`, and then use the sctLoad utility to load these files into the database.

Note **SctLoad** passes SCT information to the CWM database. You can FTP the default SCT files from the switch to the CWM workstation, and then use the **SctLoad** command to upload SCTs to CWM.

After they have been uploaded, the retrieved SCT files are displayed when you select the SCT tab which is also the default tab of the Navigator panel. Figure 7-1 shows the SCT Main window.

Figure 7-1 SCT Main window



Starting SCT

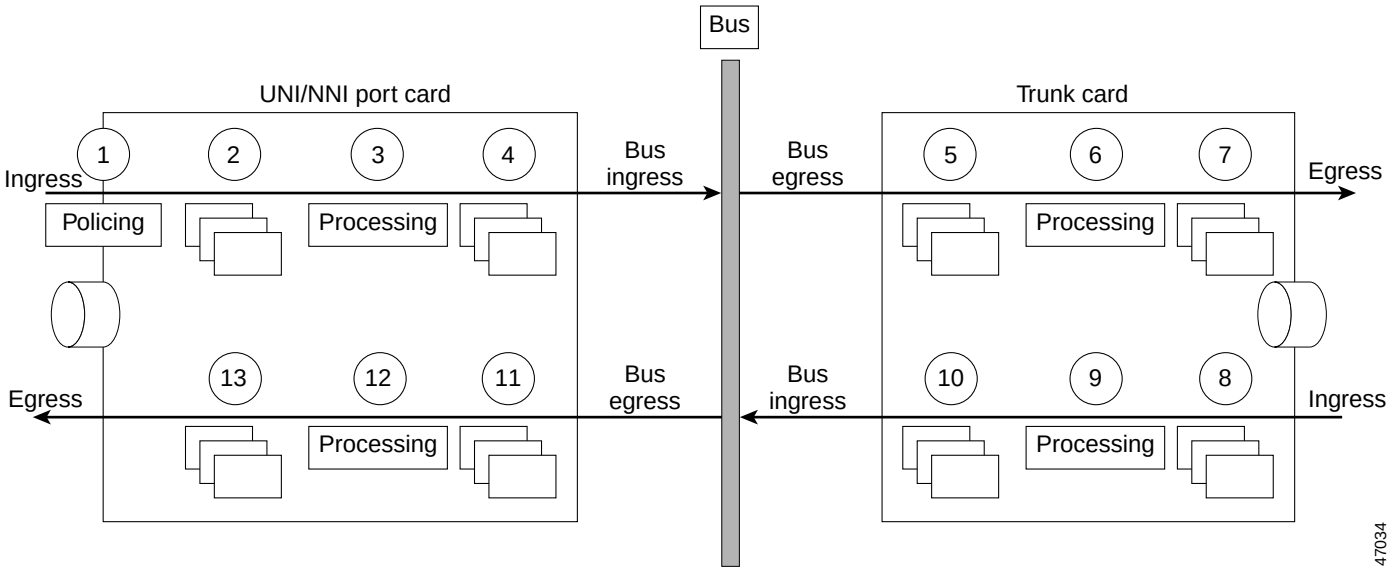
To start the SCT application, first start the CWM desktop from the CWM **Main Menu**, as described in Chapter 2, “Starting and Stopping Cisco WAN Manager.” Select **Application** from the Menu bar, and choose **Service Class Template** from the drop down menu.

Associate SCT File with Interface

The request covers both card and port association. **PORT SCT** is used for managing all traffic coming to and leaving from the port, and**CARD SCT** is used for managing all traffic coming from and leaving to the backplane of the MGX 8850.

Statistics are collected at different points during data transmission. Figure 7-2 shows how data travels through two cards that are connected across the bus.

Figure 7-2 Data Flow Through Two Cards Connected Across a Bus



The ingress direction describes traffic that travels toward the bus. The egress direction describes traffic that travels from the bus.

The numbers in Figure 7-2 correspond to the points at which statistics are collected. Points 1–7 show data on the incoming path with policing. Points 8–13 show data on the return path without policing.

- 1—Data enters the UNI/NNI port card (ingress).
- 2—Data is queued (ingress).
- 3—Data is scheduled for admission onto the bus (ingress).
- 4—Data is queued for going onto the bus (ingress).
- 5—Data is queued for being taken off the bus (egress).
- 6—Data is processed on the trunk card (egress).
- 7—Data is queued for going out the trunk (egress).
- 8—Data enters the card from the trunk (ingress).
- 9—Data is scheduled for admission onto the bus (ingress).
- 10—Data is queued for going onto the bus (ingress).
- 11—Data is queued for being taken off the bus (egress).
- 12—Data is processed on the port card (egress).
- 13—Data is queued for going out the port (egress).

Note The data flow process might vary depending on the card type.

Window Interaction

The main SCT window consists of the following:

- Menu bar
- Tool bar
- Navigator panel
- SCT tab
- Node tab
- Status bar
- Button panel
- Path label
- Data panel
  - VC panel
  - CoSB panel

Functional Interaction

The SCT GUI allows the following functions to be performed in three different ways:

- Selecting from the Options pull-down menu bar, or
- Activating a button from the tool bar, or
- Activating a button from the button panel.

Menu Bar

The Menu bar consists of **File**, **View**, and **Help** menus:

- **File** menu options (some of the following options can also be found on the Tool bar and the Button panel):
  - **New SCT GUI**: Allows an authorized user to create a new SCT GUI.
  - **New SCT File**: Allows an authorized user to create a new SCT file.
  - **Save**: The Save option allows an authorized user to modify and save a selected SCT file.
  - **Save As**: The Save As option allows an authorized user to create and save a new SCT file.
  - **Delete**: The Delete option allows an authorized user to delete a selected SCT file.
  - **Download**: The Download option allows an authorized user to load a selected SCT file.
  - **Associate**: The Associate option allows an authorized user to associate a selected SCT file.
  - **Close**: Allows an authorized user to close a selected SCT file.
  - **Exit**: Allows an authorized user to exit out of the SCT application.
- **View** menu options:
  - **Show SCT**: Shows a selected SCT file.

  - **Show Node**: Shows a selected SCT node.
- **Help** menu options:
  - **About SCT**: This feature is not available at this time.

Tool Bar

The Tool bar contains shortcut buttons to the Button panel and some File menu options:

- **Save**: The Save button allows an authorized user to modify and save a selected SCT file.
- **Save As**: The Save As button allows an authorized user to create and save a new SCT file.
- **Delete**: The Delete button allows an authorized user to delete a selected SCT file.
- **Reset**: The Reset button allows an authorized user to cancel changes and reset data for a selected SCT file.
- **Download**: The Download button allows an authorized user to load a selected SCT file.
- **Associate**: The Associate button allows an authorized user to associate a selected SCT file.

Navigator Panel

The Navigator panel consists of two tab-forms: the **SCT tab** and the **Node tab**. Each tab contains a Tree view which allows data to be visually displayed in a hierarchical file format.

The **SCT tab** is the default tab of the Navigator panel. This tab allows an authorized user to view nodes by SCT file. Nodes are displayed by expanding the SCT file node. Each SCT file can have more than one node since each SCT file can be downloaded to more than one Network node. In addition, an SCT file can also be associated by more than one Card node and more than one Port node.

The **Node tab** allows an authorized user to view SCT files by the Network node hierarchy. When Network nodes are expanded, subnodes are displayed. A Network node includes SCT file node, Card node, and Port node. If a subnode is a leaf node, then it does not have a reference and therefore can not be expanded.

In addition, when a SCT file node is selected in the Navigator panel, the SCT file data will be displayed in the Data panel. The Data panel displays VC and CoSB parameters which can be modified only if the following conditions are met:

- This SCT file is not downloaded and/or not associated with any AXSM card and /or port, and
- The user has been assigned permissions.

Note If the SCT file has been associated with a card and /or port and you want to edit the SCT, you must delete the resource partition and down the port before associating the card and /or port to the new SCT ID. After the card and/or port is associated to the new SCT ID, you can add the resource partitions again.

SCT Tab

The **SCT tab** is the default tab of the Navigator panel. In the SCT tab window, all SCT files are visually displayed in a tree format. In the SCT tab, whenever a SCT file is selected, the SCT file data is displayed in the Data Panel. If an SCT file node is not a leaf node, then it can be expanded to display Network nodes, Card nodes, and Port nodes. This expansion cycle will be repeated for each subnode that is not a leaf node:

- If the SCT file node is a leaf node and can not be expanded, then the SCT file has been created, but has not been downloaded to any Network node.
- If the Network node is a leaf node and can not be expanded, then the SCT file has been downloaded to a node, and has not been associated with any card or port of that Network node.
- If the Card node is a leaf node and can not be expanded, then the SCT file has been downloaded to the node and has been associated with the Card node. However, it has not been associated with any ports of that Card node.

Node Tab

In the **Node tab**, nodes are also displayed in a tree format. Network nodes can be expanded to view Card nodes, Port nodes, and SCT file nodes. If the Card node is not a leaf node, then it can be expanded to view the associated SCT file and its ports. The same also applies to a Port node. That is if the Port node is not a leaf node, then it can also be expanded to view the associated SCT file node.

As with the SCT Navigator view, whenever the SCT file node is selected, the SCT file data is displayed in the Data Panel.

Note that since the SCT GUI application applies only to AXSM cards, the Node view only displays AXSM cards of a Network node.

Status Bar

The Status bar is simply a label which displays the status information of the request. For example, if the modify request can not be completed because of a lock, the status bar will display the relevant error message.

Button Panel

The Button panel contains the following options: **Save**, **Save As**, **Delete**, **Reset**, **Download**, and **Associate**. (These options can also be found on the Tool bar and under the File menu options dropdown.) Buttons are enabled or disabled by the following matrix:

Table 7-1 Buttons Enable Matrix

State/Button	Save	Save As	Delete	Download	Associate
Read Only	Disable	Disable	Disable	Disable	Disable
Create State (Not Load)	Enable	Enable	Enable	Enable	Disable
Load State	Disable	Enable	Disable	Enable	Enable
Associated State	Disable	Enable	Disable	Enable	Enable

The logical sequence of loading and associating SCT files is as follows:

Create(**Save As**)->Modify(**Save**)->Load(**Download**)->**Associate**

Save As

The **Save As** button allows an authorized user to create and save a new SCT file:

Step 1 Create an SCT file by selecting **New SCT File** from the **File** dropdown menu on the main menu bar.

Step 2 Check that all Service Type tables, the CoSB table on the VC panel, and all CoSB parameters on the CoSB panel are clear.

Step 3 Select the **Save As** button from the button panel, or select **Save As** from the **File** dropdown menu.

Step 4 Name the new SCT file.

Note Newly created SCT files start at ID 100 and increment by 1 regardless of whether it is a card or port file.

Save

The **Save** button allows an authorized user to modify and save a selected SCT file. Selecting an SCT file from the SCT tab, or Node tab, will display the SCT parameters in the Main panel. If the user does not have permissions, or if the SCT file is associated, then the displaying parameters will not be modifiable. After editing parameters, press the **Save** button to save the new changes.

Delete

The **Delete** button allows an authorized user to delete a selected SCT file. The user can delete an SCT file only if it is not loaded and not associated. To delete an SCT file, select the appropriate SCT file and then press the **Delete** button.

Reset

The **Reset** button allows an authorized user to cancel changes and reset data for a selected SCT file.

Download

The **Download** button allows an authorized user to load a selected SCT file. Load an SCT file by selecting one from the SCT tab panel and pressing the **Download** button. This will prompt the user for the Node name. Once the Node ID is entered, the user selects OK to load the SCT file into the specified node.

Associate

The **Associate** button allows an authorized user to associate a selected SCT file if it has been loaded into a node. A loaded SCT file is identified by the fact that it has a leaf node on the SCT tree. Under the Node tree view, if an SCT file is a leaf node of a node, then the SCT file is loaded into that node. To associate

an SCT file, select the appropriate SCT file from the Tree panel and then press the **Associate** button. The system will prompt you for a Port or Card ID. After entering the ID, press the **OK** button to associate the SCT file.

SCT Deletion

The SCT manager only allows the deletion of a non-downloaded SCT file. If the SCT file has been downloaded to the switch or node, it can only be removed or deleted using the "delsct" CLI command.

Path Label

The Path label gives the location of the selected SCT Card or Port file.

Data Panel

The **Data panel** displays the SCT data of associated VC parameters and CoSB parameters. These parameters are displayed in two sub-panels: a VC panel and a CoSB panel. The VC panel contains both VC parameters and CoSB parameters in a table format. The CoSB panel displays only CoSB parameters.

VC Panel

The **VC panel** is organized into a series of tab panes. Each tab represents a group of VC parameters which categorically belong to that group. In addition, there are two tabs of which one displays all VC parameters and the other displays all CoSB parameters. Currently, there are a total of eight tabs, and each tab represents a group as follows:

Policy: Displays information related to management priorities for network traffic

- Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- Cosb Number: The Class of Service Buffer number associated with the service type. Access: read-write. Values: 1-16.
- CAC Treatment: Connection Admission Control. The CAC algorithms that are supported are: 1) lcnCac, 2) eCac-Model A, 3) eCac-Model B, 4) eCac-Model C, 5) eCac-Model D, 6) eCac-Model E, 7) eCac-Model F, 8) mbBwCac. DEFVAL {2}. Access: read-write. Values: 1-256.
- UPC Enable: When a connection is added, a VPI.VCI address is assigned, and UPC parameters are configured for the connection. For each cell in an ATM stream, the VPI.VCI addresses are verified and each cell is checked for compliance with UPC parameters.
- UPC CLP: Usage Parameter Control- Cell Loss Priority Select. Disable GCRAs and GCRA #2 with Packet Policing Action are used for policing packet or frame traffic. GCRA1-ENB: Enables GCRA1 only. GCRA 1&2: Enables you to turn on policing for one or both GCRA1 & GCRA2.

- GCRA-1: Indicates the handling of cells that fail the first (PCR) bucket of the policer. If object UPC_ENABLE is set to *disable the policing*, then this object is not used. Options for this feature include: 1- Discard, 2- Set CLP bit, 3- Set CLP of untagged cells, discard tagged cells.
- GCRA-2: Indicates the handling of cells that fail the second (PCR) bucket of the policer. If object UPC_ENABLE is set to *disable the policing*, then this object is not used. Options for this feature include: 1- Discard, 2- Set CLP bit, 3- Set CLP of untagged cells, discard tagged cells.

Conn Parm: Displays information related to connection types, services and categories

- Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- Peak Cell Rate (PCR): The peak (maximum) cell rate for a connection using this service type. This value is a percentage of the maximum cell rate for the logical interface. 1000000 is equal to 100%. Range and Units: 0-1000000.
- Sustained Cell Rate (SCR): The sustained cell rate for a connection using this service type. This value is a percentage of the PCR. 1000000 is equal to 100%. Range and Units: 0-1000000.
- Min Cell Rate (MCR): The minimum cell rate for a connection using this service type. This value is a percentage of the PCR. 1000000 is equal to 100%. Range and Units: 0-1000000.
- ICR: Initial Cell Rate. The cell rate used to begin a transmission on a connection that has been idle for a configured period of time. This value is a percentage of the PCR for the logical interface. 1000000 is equal to 100%. (Used only on ABR service type connections.) Range and Units: 0-1000000.
- MBS: Max Burst Size. The maximum number of cells that may arrive at a rate equal to the PCR. Used for policing. Range and Units: 1-500000.
- MFS: Max Frame Size. The maximum AAL5 frame size in cells.
- CDVT: Cell Delay Variation Tolerance for the first leaky bucket.
- Packet Discard Mode: Enables or disables Packet Discard Mode on the connection. Range and units: 1=enabled; 2=disabled.

VC Threshold: Displays information related to the Virtual Channel Threshold

- Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- Maximum Threshold: The VcMax Threshold for CLP (0+1) cells in microseconds. Range and units: 0-5000000 microseconds.
- CLP (1) High Threshold: Cell Loss Priority High Threshold (% of VC QMax) is the highest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions. Most often set by the ingress policing function.
- CLP-LOW/EPD1: CLP (1) Low or EPDs (1): Cell Loss Priority Low Threshold (% of VC QMax)/ Early Packet Discard. If AAL5 FBTC = yes, then for the BXM card this is the EPD threshold setting. EPDs is the lowest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions.

- EPD0: Early Packet Discard Threshold. The maximum threshold for CLP (0+1) cells. This value is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and value: 0-1000000.
- EFCI Threshold: Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.

Scaling: Displays information related to Service Scaling

- Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- COS Scaling: Class of Service Scaling: Class of Service Scaling provides a means of scaling through a set of extended parameters, which are generally platform specific, based on a set of standard ATM parameters passed to the VSI slave during connection set up.
- Interface Scaling: Allows the scaling and exchange of information between connections.

ABR: Displays information related to the ABR Service Type

- Service Type: ABR (Available Bit Rate) service type and parameters.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- CI Control: Congestion Indicator is a field in an RM-cell used to cause the source to decrease its ACR (Allowed Cell Rate). The source sets CI =0 when it sends an RM cell. C=1indicats EFCI has been received on a previous data cell.
- Cut-Off RM Cells: Allows for variations in the RM-cell.
- VSVD: Virtual Source/ Virtual Destination. A VSVD is an ABR connection which may be divided into two or more separately controlled ABR segments. Each ABR control segment, except the first, is sourced by a virtual source. Sources and destinations are linked via bi-directional connections, and each connection termination point is both a source and a destination, a source for data that is transmitting, and a destination for data that is receiving.
- ADTF: Allowed-cell-rate Decrease Time Factor/Initial-cell-rate Time-out. The time between RM cells before the allowable cell rate returns to the initial cell rate.
- RDF: Rate Decrease Factor: An ABR service parameter that controls the decrease in cell transmission rate.
- RIF: Rate Increase Factor. A percentage increase in the allowable cell rate for an ABR connection if the BRM cells do not have the N1 or C1 bits set.
- NRM: Number RM. The maximum number of data cells that can be sent before sending an RM cell on an ABR connection.
- TRM: Time RM/Minimal Adjustment Period. The maximum amount of time between RM cells on an ABR connection.
- CDF: Cutoff Decrease Factor. CDF controls the decrease in ACR (Allowed Cell rate), which is an ABR service parameter, associated with CRM (Cell Rate Margin), which is a measure of the difference between the effective bandwidth allocation and the allocation for sustainable rate in cells per second.

- TBE: Transient Buffer Exposure. The number of RM cells that can be sent out by a virtual source before waiting for a BRM cell in return.
- FRTT: FRTT(millisec): Fixed Round-Trip Time. The amount of delay expected for an RM cell to travel through the network to the destination and back again.

WFQ: Displays information related to Weighted Fair Queuing

- Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- WFQ: Weighted Fair Queuing. WFQ queues traffic in separate queues, according to traffic class definition, guaranteeing each queue some portion of the total available bandwidth. WFQ recognizes when a particular queue is not fully utilizing its allocated bandwidth and portions that capacity out to the other queues on a proportionate basis. This is done by portioning out available bandwidth on the basis of individual information flows according to their message parameters.

All VC: Displays information related to All VC

- Service Type: The service type (i.e. CBR, VBR, ABR) to which the parameters apply.
- Service Category: The service category to which the service type belongs. All service types that belong to the same service category should be mapped to the same Class of Service Buffer. Access: read only. Values: 0-65535.
- CoSB No: Class of Service Buffer Number. The number that identifies one of the sixteen Cosb buffers. A Cosb buffer is a buffer that services connections with similar QoS requirements. Range and units:1-16.
- CAC Treatment: Connection Admission Control. The CAC algorithms that are supported are: 1) lcnCac, 2) eCac-Model A, 3) eCac-Model B, 4) eCac-Model C, 5) eCac-Model D, 6) eCac-Model E, 7) eCac-Model F, 8) mbBwCac. DEFVAL {2}. Access: read-write. Values: 1-256.
- UPC Enable: When a connection is added, a VPI.VCI address is assigned, and UPC parameters are configured for the connection. For each cell in an ATM stream, the VPI.VCI addresses are verified and each cell is checked for compliance with UPC parameters.
- UPC CLP: Usage Parameter Control- Cell Loss Priority Select. Enables or disables GCRA policing functions on the connection. GCRA1-ENB: Enables GCRA1 only. GCRA 1&2: Enables both GCRA1 & GCRA2. Options for this feature include: 1- Bk 1: CLP (0+1); Bk 2: CLP (0), 2- Bk 1: CLP (0+1); Bk 2: CLP (0+1), 3- Bk 1: CLP (0+1); Bk 2: Disabled, 4- Bk 1: CLP (0+1) with MFS.
- GCRA-1: Indicates the handling of cells that fail the first (PCR) bucket of the policer. If object UPC_ENABLE is set to *disable the policing*, then this object is not used. Options for this feature include: 1- Discard, 2- Set CLP bit, 3- Set CLP of untagged cells, discard tagged cells.
- GCRA-2: Indicates the handling of cells that fail the second (PCR) bucket of the policer. If object UPC_ENABLE is set to *disable the policing*, then this object is not used. Options for this feature include: 1- Discard, 2- Set CLP bit, 3- Set CLP of untagged cells, discard tagged cells.
- PCR: The peak (maximum) cell rate for a connection using this service type. This value is a percentage of the maximum cell rate for the logical interface. 1000000 is equal to 100%. Range and Units: 0-1000000.
- SCR: The sustained cell rate for a connection using this service type. This value is a percentage of the PCR. 1000000 is equal to 100%. Range and Units: 0-1000000.

- MCR: The minimum cell rate for a connection using this service type. This value is a percentage of the PCR. 1000000 is equal to 100%. Range and Units: 0-1000000.
- ICR: Initial Cell Rate. The cell rate used to begin a transmission on a connection that has been idle for a configured period of time. This value is a percentage of the PCR for the logical interface. 1000000 is equal to 100%. (Used only on ABR service type connections.) Range and Units: 0-1000000.
- MBS: The maximum number of cells that may arrive at a rate equal to the PCR. Used for policing. Range and Units: 1-500000.
- MFS: Max Frame Size. The maximum AAL5 frame size in cells.
- CDVT: Cell Delay Variation Tolerance for the first leaky bucket.
- Packet Discard Mode: Enables or disables Packet Discard Mode on the connection. Range and units: 1=enabled; 2=disabled.
- Maximum Threshold: The VcMax Threshold for CLP (0+1) cells in microseconds. Range and units: 0-5000000 microseconds.
- CLP-HIGH: Cell Loss Priority High Threshold (% of VC QMax) is the highest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions. Most often set by the ingress policing function. Range and values: 0-1000000.
- CLP-LOW/EPD1: CLP (1) Low or EPDs (1): Cell Loss Priority Low Threshold (% of VC QMax)/ Early Packet Discard. If AAL5 FBTC = yes, then for the BXM card this is the EPD threshold setting. EPDs is the lowest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions.
- EPD0: Early Packet Discard Threshold. The maximum threshold for CLP (0+1) cells. This value is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and value: 0-1000000.
- EFCI: Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.
- CoS Scaling: Class of Service Scaling provides a means of scaling through a set of extended parameters, which are generally platform specific, based on a set of standard ATM parameters passed to the VSI slave during connection set up.
- Interface Scaling: Allows the scaling and exchange of information between connections.
- CI Control: Congestion Indicator is a field in an RM-cell used to cause the source to decrease its ACR (Allowed Cell Rate). The source sets CI =0 when it sends an RM cell. C=1indicats EFCI has been received on a previous data cell.
- Cut-Off RM Cells: Allows for variations in the RM-cell.
- VSVD: Virtual Source/ Virtual Destination. A VSVD is an ABR connection which may be divided into two or more separately controlled ABR segments. Each ABR control segment, except the first, is sourced by a virtual source. Sources and destinations are linked via bi-directional connections, and each connection termination point is both a source and a destination, a source for data that is transmitting, and a destination for data that is receiving.
- ADTF: Allowed-cell-rate Decrease Time Factor/Initial-cell-rate Time-out. The time between RM cells before the allowable cell rate returns to the initial cell rate.
- RDF: Rate Decrease Factor: An ABR service parameter that controls the decrease in cell transmission rate.

- RIF: Rate Increase Factor. A percentage increase in the allowable cell rate for an ABR connection if the BRM cells do not have the N1 or C1 bits set.
- NRM: Number RM. The maximum number of data cells that can be sent before sending an RM cell on an ABR connection.
- TRM: Time RM/Minimal Adjustment Period. The maximum amount of time between RM cells on an ABR connection.
- CDF: Cutoff Decrease Factor. CDF controls the decrease in ACR (Allowed Cell rate), which is an ABR service parameter, associated with CRM (Cell Rate Margin), which is a measure of the difference between the effective bandwidth allocation and the allocation for sustainable rate in cells per second.
- TBE:Transient Buffer Exposure. The number of RM cells that can be sent out by a virtual source before waiting for a BRM cell in return.
- FRTT: Fixed Round-Trip Time. The amount of delay expected for an RM cell to travel through the network to the destination and back again.
- WFQ: Weighted Fair Queuing is an approximation of the Generalized Processor Sharing (GPS) scheduling. WFQ can be generally used to give performance guarantees to connections carrying best-effort packet traffic, where each connection can be guaranteed bandwidth in proportion to its weight and in a fair manner.

All CoSB: Presents all CoSB information within the VC panel display

- CoSB No: Class of Service Buffer Number. The number that identifies one of the sixteen Cosb buffers. A Cosb buffer is a buffer that services connections with similar QoS requirements. Range and units:1-16.
- Minimum Rate: Min Cell Rate (MCR): Set to default value. This field is not editable.
- Maximum Rate: Peak Cell Rate (PCR). Set to default value. This field is not editable.
- Minimum Priority: The priority at which this COSB will be serviced to guarantee it minimum and maximum bandwidth requirements. Highest priority = 0; Lowest priority = 15. Range and units: 0-15.
- Excess Priority: The priority at which this COSB will be given access to excess bandwidth. Highest priority = 0; Lowest priority = 15. Range and units: 0-15.
- Maximum Threshold:The VcMax Threshold for CLP (0+1) cells in microseconds. Range and units: 0-5000000 microseconds.
- CLP-HIGH: Cell Loss Priority High Threshold (% of VC QMax) is the highest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions. Most often set by the ingress policing function. Range and values: 0-1000000.
- CLP-LOW/EPD1: CLP (1) Low or EPDs (1): Cell Loss Priority Low Threshold (% of VC QMax)/ Early Packet Discard. If AAL5 FBTC = yes, then for the BXM card this is the EPD threshold setting. EPDs is the lowest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions.
- EPD0 Threshold: Early Packet Discard Threshold. The maximum threshold for CLP (0+1) cells. This value is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and value: 0-1000000.
- EFCI Threshold: Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.

- Explicit Rate Sampling: Indicates whether Explicit Rate Sampling (ERS) is enabled or disabled. Range and units: 1=enabled; 2=disabled.
- Random Early Discard Selection(RED): RED will drop packets from queues on a random basis in order to avoid buffer overflow. RED is accomplished by dropping packets on a random basis, which is determined statistically, when the mean queue depth exceeds a threshold over a period of time, effectively advising the packet source router to decrease its packet rate.
- RED Threshold: Random Early Discard Threshold: The threshold at which the COSB Random Early Discard (RED) is activated. This threshold is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and units: 0-1000000.
- RED Probability: Random Early Discard Probability Factor: The mantissa value of probability for maximum discard when RED is activated. Determined as 1/2^<value>.
- WFQ: Weighted Fair Queuing. WFQ queues traffic in separate queues, according to traffic class definition, guaranteeing each queue some portion of the total available bandwidth. WFQ recognizes when a particular queue is not fully utilizing its allocated bandwidth and portions that capacity out to the other queues on a proportionate basis. This is done by portioning out available bandwidth on the basis of individual information flows according to their message parameters.
- Best Effort: A Quality of Service Class in which no specific traffic parameters and no absolute guarantees are provided. Best Effort includes UBR and ABR Service Types.
- Discard Alarm Enable: Indicates whether Discard Alarm has been enabled or disabled. Range and units: 1=enabled; 2=disabled.
- Discard Alarm Threshold: Indicates the Discard Alarm Threshold.
- Cell Loss Ratio: A negotiated Quality of Service parameter in an ATM network. This parameter indicates a ratio of lost cells to total transmitted cells.

Each tab displays parameters in table format, with the above criteria and its associated data presented in each column of a given table. Each row represents a unique Service Type, including: ABR, CBR, UBR, VBR and VSI Signal.

By selecting a row on the table, the corresponding CoSB parameters are also displayed in the bottom CoSB panel.

Except for Service Type and Service Category columns, most columns under each VC tab have drop down boxes which allow authorized users to edit and modify cells as needed.

Cells are editable and can be changed ONLY if both of the following conditions are met:

- The user has security permissions to configure SCT files, and
- The SCT file is not downloaded and/or not associated

CoSB Panel

The CoSB panel displays CoSB parameters by CoSB Number. The data in this panel reflects the row selection of the table on the VC or top panel. These parameters are currently organized into three groups: Rate & Priority, Threshold, and Miscellaneous.

In the **Rate & Priority** category, the following parameters can be modified:

- Minimum Rate: The minimum rate at which this COSB will be serviced in order to guarantee its minimum and maximum bandwidth requirements.
- Maximum Rate: The minimum rate at which this COSB will be serviced in order to guarantee its minimum and maximum bandwidth requirements.

- Minimum Priority: The priority at which this COSB will be serviced to guarantee its minimum and maximum bandwidth requirements. Highest priority = 0; Lowest priority = 15. Range and units: 0-15.
- Excess Priority: The priority at which this COSB will be given access to excess bandwidth. Highest priority = 0; Lowest priority = 15. Range and units: 0-15.

In the **Threshold category**, the following parameters can be modified:

- Maximum: Maximum Threshold.
- CLP High: Cell Loss Priority High Threshold (% of VC QMax) is the highest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions. Most often set by the ingress policing function.
- CLP Low: Cell Loss Priority Low Threshold (% of VC QMax) is the lowest threshold for the bit in the header of an ATM cell that identifies the cell as eligible for discard within the network under predefined congestion conditions.
- EPD0: Early Packet Discard Threshold. The maximum threshold for CLP (0+1) cells. This value is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and value: 0-1000000.
- EFCI Threshold: Explicit Forward Congestion Indication. The VC EFCI discard threshold. This value is a percentage of MAX_CELL THRESH. 1000000 is equal to m100%. Range and values: 0-1000000.
- RED: Random Early Discard. The threshold at which the COSB Random Early Discard (RED) is activated. This threshold is a percentage of the MAX_CELL THRESH for the connection. 1000000 is equal to 100%. Range and units: 0-1000000.
- Dscd Alm Th: Indicates the Discard Alarm Threshold.

In the **Miscellaneous category**, the following parameters can be modified:

- RED Pro Factor: Random Early Discard Probability Factor. The mantissa value of probability for maximum discard when RED is activated. Determined as 1/2^<value>.
- RED Selection: Random Early Discard will drop packets from queues on a random basis in order to avoid buffer overflow. RED is accomplished by dropping packets on a random basis, which is determined statistically, when the mean queue depth exceeds a threshold over a period of time, effectively advising the packet source router to decrease its packet rate.
- WFQ: Weighted Fair Queuing is an approximation of the Generalized Processor Sharing (GPS) scheduling. WFQ can be generally used to give performance guarantees to connections carrying best-effort packet traffic, where each connection can be guaranteed bandwidth in proportion to its weight and in a fair manner.
- ERS: Explicit Rate Stamping. Indicates whether Explicit Rate Stamping (ERS) is enabled or disabled. Range and units: 1=enabled; 2=disabled.
- Best Effort: A Quality of Service Class in which no specific traffic parameters and no absolute guarantees are provided. Best Effort includes UBR and ABR Service Types.
- Dscrd Alarm: Enable/disable Discard Alarm per VC: Indicates whether Discard Alarm has been enabled or disabled. Range and units: 1=enabled; 2=disabled.
- CLR- Cell Loss Ratio. CLR is a negotiated QoS (Quality of Service) parameter and acceptable values are network specific. The objective is to minimize CLR provided the end-system adapts the traffic to the changing ATM layer transfer characteristics. The CLR is defined for a connection as Lost Cells/Total Transmitted Cells.

If you select a different CoSB number by selecting another row from the table of the top panel, the data on this panel will simultaneously change to reflect your selection.

In addition, when you move from one tab to the next, the data on this panel will simultaneously change if the CoSB number has also been changed.

As with the VC parameters, the CoSB parameters can also be changed only if both of the following conditions are met:

- The user has security permissions to configure SCT files, and
- The SCT file is not downloaded and/or not associated.

Creating a New Service Class Template

Service Class Templates can only be modified or created using the Cisco WAN Manager (CWM). The following explains how to use CWM to create your own SCTs.

Caution Only network engineers who are extremely knowledgeable about ATM and its parameters should create and use their own SCTs.

Creating a new SCT involves configuring the ATM parameters for specific classes of service to suit the special needs of your customers. For example, if you have customers with special policing or nonpolicing requirements, you can create an SCT to meet those specifications.

Some service providers offer different levels of service (such as gold, silver, or bronze) at different prices. Each level of service offers a different class of service and is supported by a different SCT.

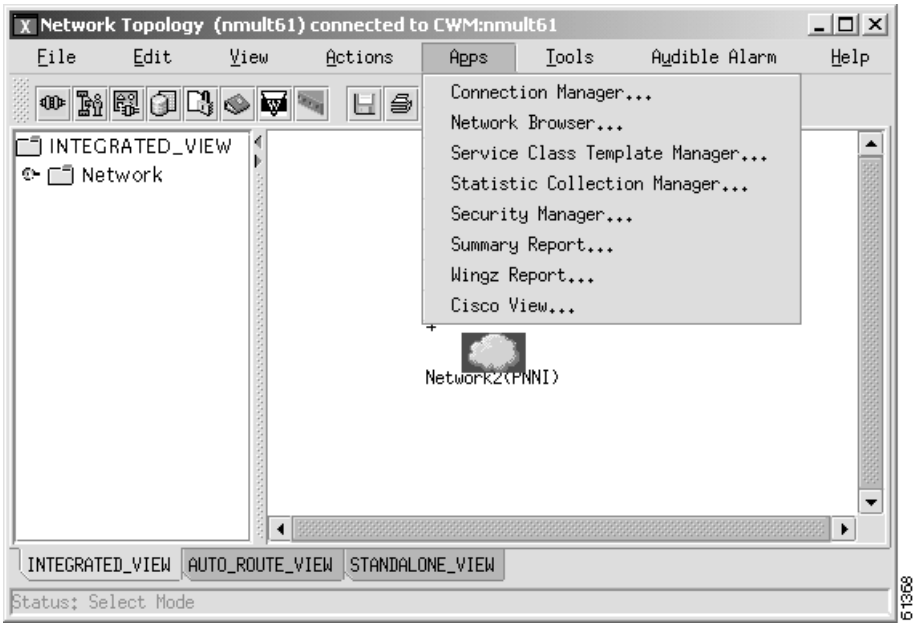
Launching the Service Class Template Manager

The Service Class Template Manager can be launched from the toolbar by clicking on the Service Class Template Manager icon as shown in Figure 7-3.

Figure 7-3 Close-up of Service Class Template Manager icon

Figure 7-4 shows the **CWM Apps Menu View**. The Service Class Template Manager can also be launched from the **Apps** menu by clicking on **Apps** and selecting **Service Class Template Manager**.

Figure 7-4 CWM Apps Menu view



Navigating the Service Class Template Manager

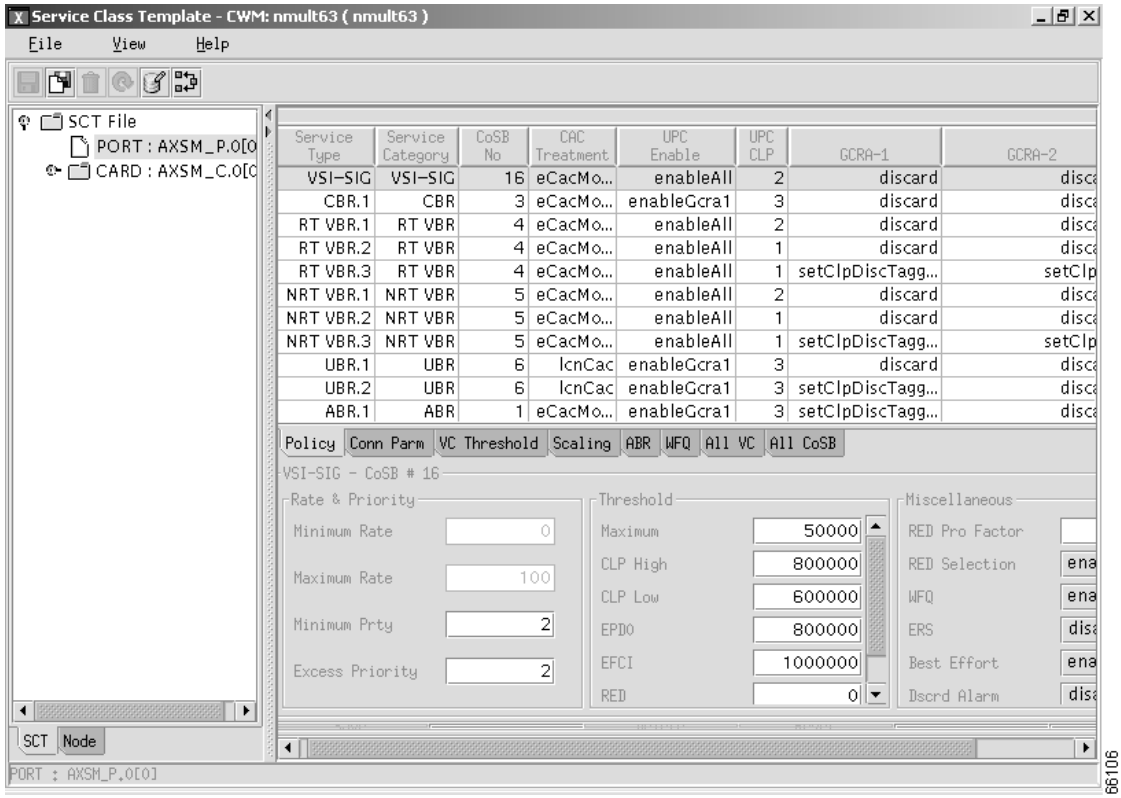
Figure 7-5 shows the Service Class Template Manager. In the left column, under **SCT File**, the SCTs that are available on the card are listed. This view shows two SCTs:

- **PORT : AXSM_EGR0[0]**
- **CARD : AXSM_ING[0]**

The PORT SCT is used for managing all the traffic that is entering into and leaving from the port, while the CARD SCT is used for managing all the traffic entering into and leaving the backplane of the MGX 8850.

PORT : AXSM_EGR0[0] is highlighted.

Figure 7-5 Service Class Template Manager with Policy selected

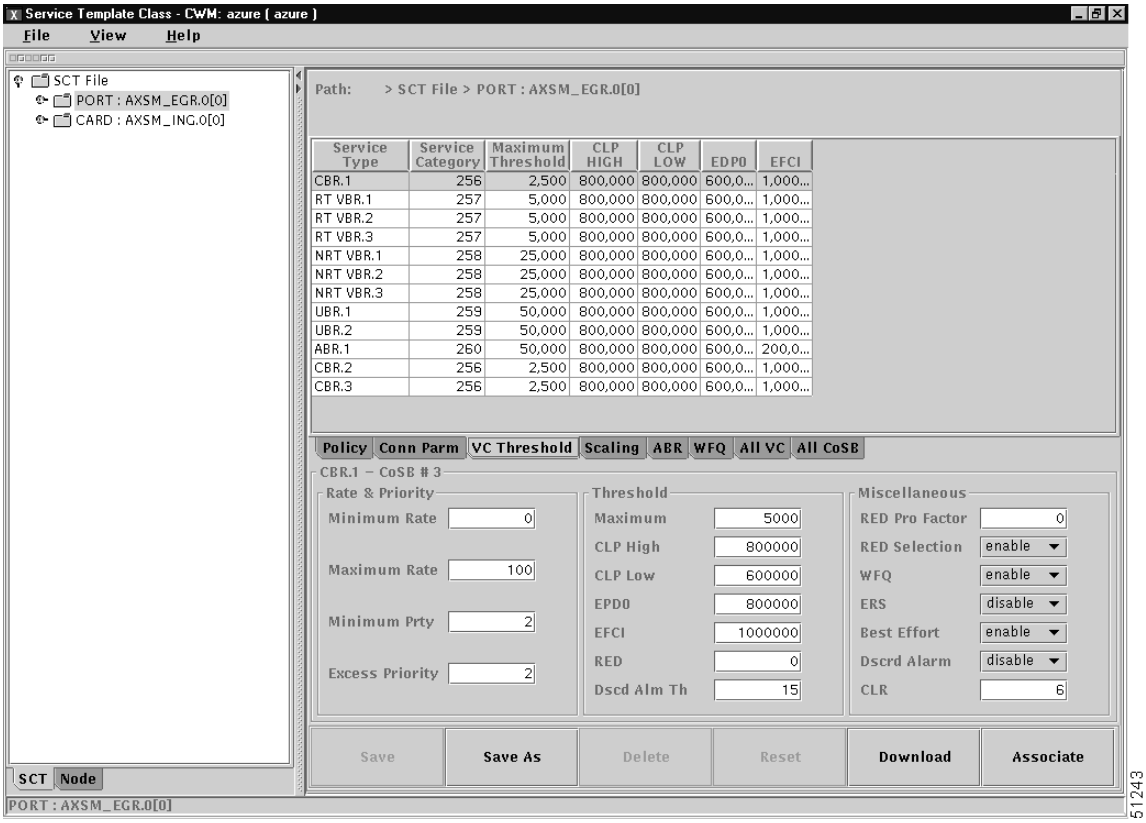


SCT parameters can be added or changed using either the SCT Tables or the SCT Entry Fields.

SCT Tables

The SCT Tables are the white rows and columns that appear in the upper half of the SCT Manager Window. To display different parameter tables, select one of the other tabs, such as **Conn Parm** or **VC Threshold**. For example, Figure 7-6 shows the Service Class Template Manager with the **VC Threshold** tab selected.

Figure 7-6 Service Class Template Manager with VC Threshold Selected



Entry Fields

The Entry Fields appear in the gray, lower half of the SCT Manager Window. When you select a Service Type in the SCT Table, the name of the Service Type appears over the Entry Fields section and the CosB parameters for that Service Type appear in the Entry Fields.

Changing SCT Parameters

SCT Parameters can be modified using either a table or an entry field. The SCT tables contain all parameters, while the entry fields display only the most frequently accessed parameters.

Using the SCT Tables

To change an SCT parameter using the SCT Tables, select and highlight the field of the parameter you want to change by double-clicking on it. Once the field is selected you can either type a new number into the field or select a new value from a pull-down menu. Most fields have pull-down menus, but some require that the new value be typed.

The SCT Tables are the white rows and columns that appear in the upper half of the SCT Manager Window. The rows are the service types, and the columns are the parameters. Different parameter tables are displayed by selecting one of the different table tabs. The table tabs run horizontally through the middle of the SCT Manager. Figure 7-7 shows a chosen service category field with the Policy tab selected.

Figure 7-7 SCT Manager with a Service Category Field selected

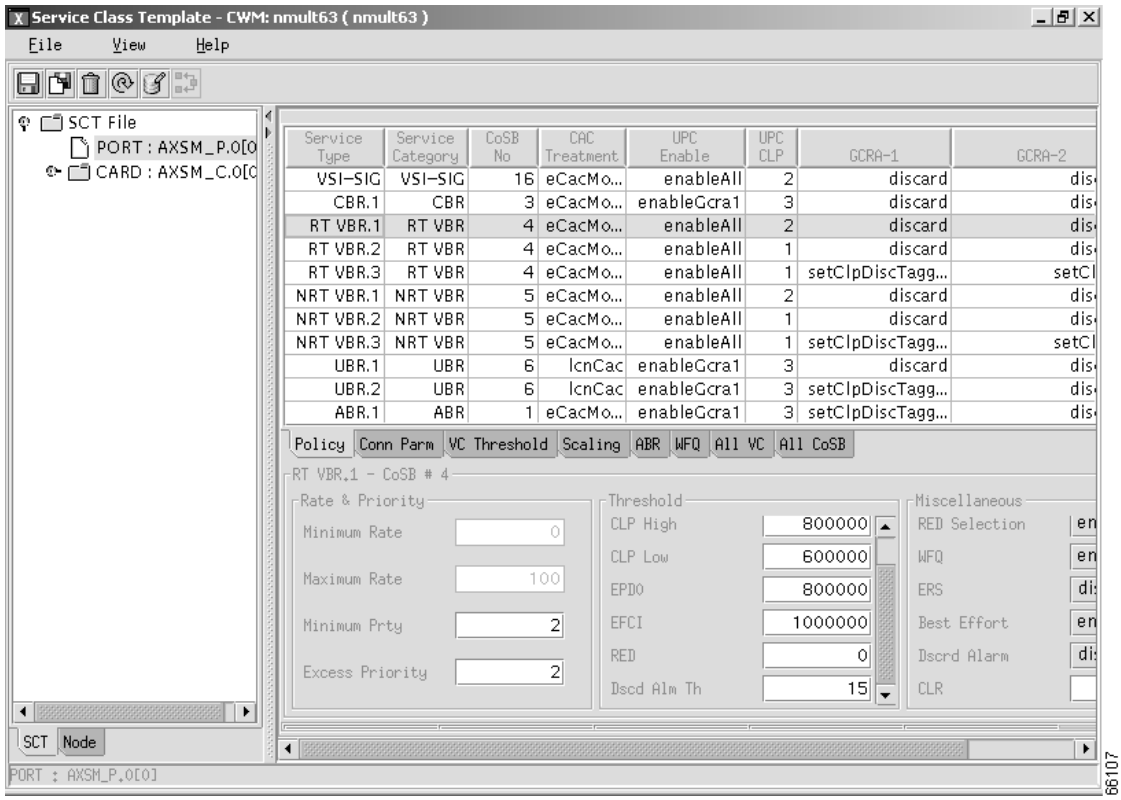
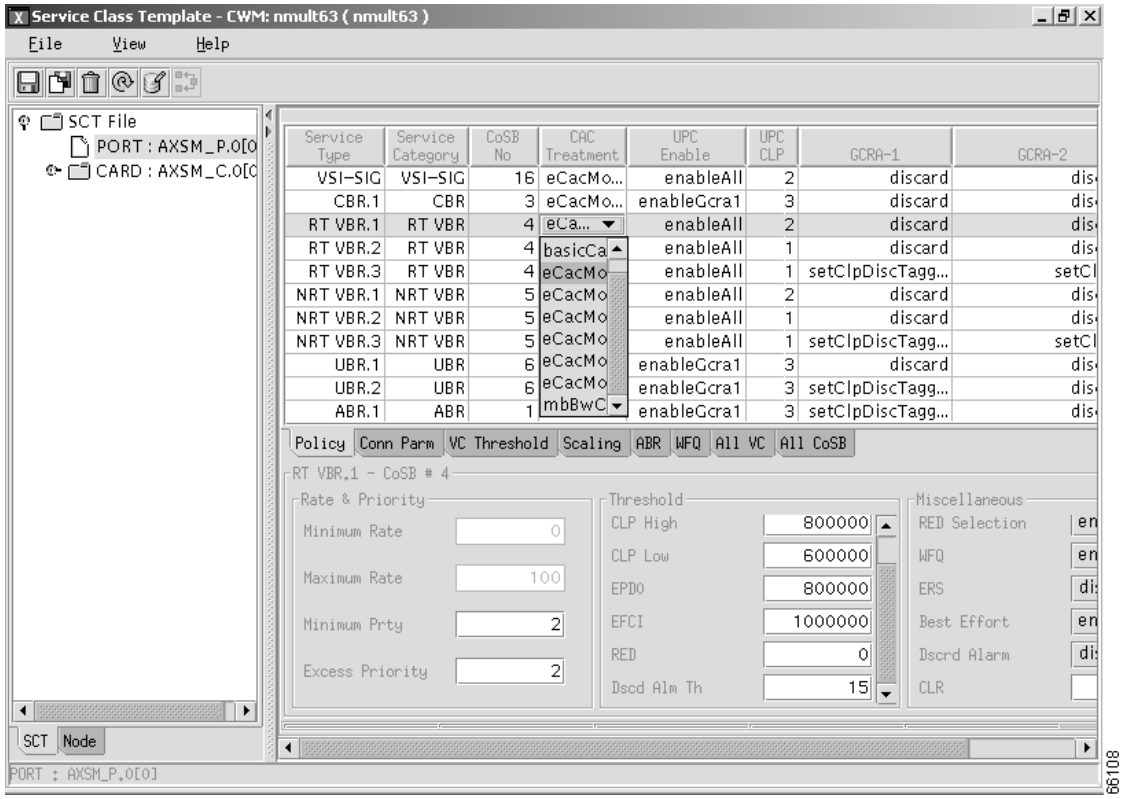


Figure 7-8 shows the SCT Manager with the CAC Treatment field for RT VBR.1 selected and the pull-down menu displayed. To change this value, select a different value from the pull-down menu.

Figure 7-8 SCT Manager with CAC Treatment field selected



Using the Entry Fields

When you select a Service Type in the SCT Table, the name of the Service Type appears over the Entry Fields section and the CosB parameters for that Service Type appear in the Entry Fields.

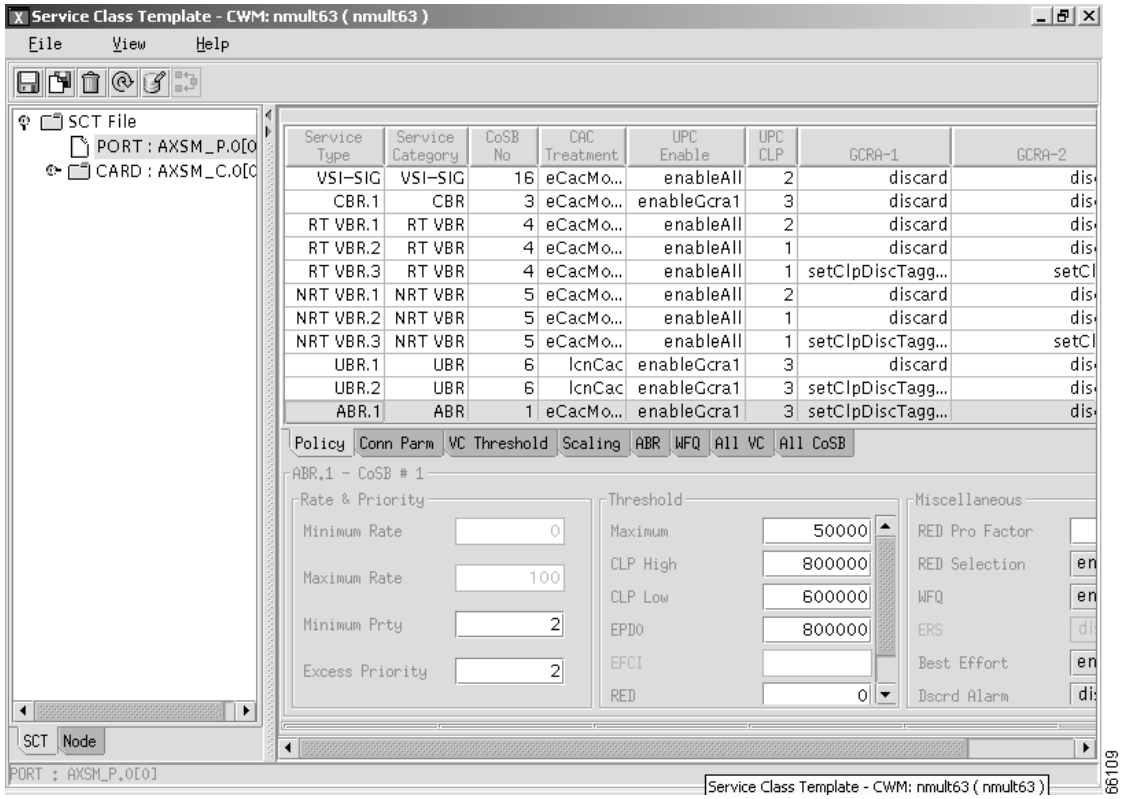
The Entry Fields are divided into three columns:

- Rate and Priority
- Threshold
- Miscellaneous

Figure 7-9 shows the SCT Manager with ABR.1 selected. *ABR.1 - CosB #1* appears over the Entry Fields section. 100 in the Maximum Rate field of the Rate and Priority column is highlighted in blue.

To change a parameter in an entry field, select and highlight the field of the parameter you want to change by double-clicking on it. Then, type in the new value.

Figure 7-9 SCT Manager with ABR.1 Selected



Reset Button

The **RESET** button resets all of the SCT fields to their saved settings.

Associate Button

The ASSOCIATE button allows you to select a network.To associate an SCT file, select the appropriate SCT file from the Tree panel and then press the **Associate** button. Pressing the **Associate** button opens a dialog box prompting you for a Port or Card ID. After entering the ID, press the **OK** button to associate the SCT file.

Saving a New or Modified SCT

To save a new or modified SCT, click the **Save** or **Save As** button in the lower left corner of the SCT Manager. Enter a new name and press enter.

SCT Refresh

After you save a changed SCT file, the SCT manager screen is Not automatically updated or refreshed. You MUST refresh the screen manually in the following manner:

Step 1 Select the root node SCT file

Note On the SCT tab, the root node name is "SCT File"; on the Node tab, the root node name is "Network".

Step 2 Verify by observing that the tree view has discarded tree nodes and retrieved updated data from the CWM database.

Note For the SCT tab, the refresh also occurs when *any* SCT file is selected and is followed by a closing of the magnifying glass or collapsing of the root node. Only after re-expanding the root node will the SCT be refreshed.

Downloading a New SCT

To download an SCT, click on the **DOWNLOAD** button and follow the instructions in the **Download** dialog box.

Verifying that a New SCT is Loaded

To verify that an SCT is loaded, use the following procedure.

Step 1 Login to the switch and go to the C:SCT/AXSM directory.

Step 2 To get to the C:SCT/AXSM directory, type **pwd** (Present Working Directory) at the controller (PXM) prompt. This puts you at the C: directory.

```
pop20two.7.PXM.a > pwd
C:
```

Step 3 Change to the SCT directory by typing **cd** SCT.

```
pop20two.7.PXM.a > cd SCT
```

Step 4 Change to the AXSM directory by typing **cd** AXSM.

```
pop20two.7.PXM.a > cd AXSM
```

Step 5 Display the contents of the AXSM directory by typing **ls** or **ll**.

```
pop20two.7.PXM.a > ll
size date time name
-------- ------ ------ --------
512 NOV-17-2000 20:04:28 . <DIR>
512 NOV-17-2000 20:04:28 .. <DIR>
6910 NOV-17-2000 20:04:28 AXSM_SCT.CARD.7
```

```
6910 NOV-17-2000 20:04:30 AXSM_SCT.PORT.7
7212 NOV-17-2000 20:04:30 AXSM_SCT.CARD.2
7212 NOV-17-2000 20:04:30 AXSM_SCT.CARD.3
7212 NOV-17-2000 20:04:30 AXSM_SCT.PORT.2
7212 NOV-17-2000 20:04:30 AXSM_SCT.PORT.3

In the file system :
total space : 819200 K bytes
free space : 702351 K bytes
```

Note The following is an example of the directory output for an AXSM-E that is displayed by typing **ls** or **ll**.

```
size          date       time       name
--------       ------     ------    --------
     512    AUG-17-2001  01:22:04   .
     512    AUG-17-2001  01:22:04   ..
    7212    JUL-11-2001  02:44:30   AXSM_SCT.CARD.2
    7212    JUL-11-2001  02:44:30   AXSM_SCT.PORT.2
    7212    JUL-11-2001  02:44:30   AXSM_SCT.CARD.3
    7212    JUL-11-2001  02:44:32   AXSM_SCT.PORT.3
    7212    JUL-11-2001  02:44:32   AXSM_SCT.CARD.100
    9957    AUG-09-2001  19:47:44   AXSME_SCT.CARD.101
    7212    JUL-11-2001  02:44:32   AXSM_SCT.PORT.102
    7212    JUL-11-2001  02:44:32   AXSM_SCT.PORT.110
    7211    JUL-11-2001  02:44:32   AXSM_SCT.PORT.121
    7155    JUL-11-2001  02:44:32   AXSM_SCT.PORT.123
    8029    JUL-11-2001  02:44:32   AXSM_SCT.PORT.134
    9957    AUG-03-2001  18:48:02   AXSM_SCT.PORT.4
    9957    AUG-03-2001  18:48:14   AXSM_SCT.PORT.5
    9957    AUG-03-2001  18:48:02   AXSM_SCT.CARD.4
    9957    AUG-03-2001  18:48:14   AXSM_SCT.CARD.5
    7212    JUL-11-2001  02:44:32   AXSM_SCT.PORT.100
    9957    AUG-09-2001  19:48:08   AXSM_SCT.CARD.102
    7211    JUL-11-2001  02:44:32   AXSM_SCT.CARD.103
    7211    JUL-11-2001  02:44:32   AXSM_SCT.PORT.113
    7212    JUL-24-2001  01:34:42   AXSM_SCT.PORT.101
    9957    AUG-16-2001  18:52:48   AXSME_SCT.CARD.5
    9957    AUG-16-2001  18:52:54   AXSME_SCT.PORT.5
    9957    AUG-09-2001  19:48:22   AXSME_SCT.PORT.103
    9957    AUG-17-2001  01:22:06   AXSM_SCT.PORT.104
   10317    AUG-17-2001  18:54:54   AXSME_SCT.PORT.6

In the file system :
    total space : 819200 K bytes
    free  space : 690456 K bytes
```

Step 6 Verify that the name of the SCT you are looking for is in the list.

Note CWM will select SCTs by first sorting SCTs using capital letters and then sorting SCTs using lower case letters. (i.e. AXSM_SCT.CARD.2 would be selected before axsm_sct.card.2). Be aware of this when creating a new file name or when sending a file via FTP.

Note The CWM SCT manager will select IDs starting at ID 100 and increment by one until it reaches ID 255. The SCT ID numbers are automatically assigned and automatically associated with the SCT template file name(s).

SCT Manager Maintenance

The following procedures are used to rebuild SCT manager after a coldstart -F. This rebuild of the SCT manager could be required after uploading all SCT files, and before creating new SCT files.

Statistics Collection Manager

The Statistics Collection Manager (SCM) for Release 10 of CWM features two types of Statistics Collection Management. One type of SCM is installed as part of the CWM Server installation on the CWM server workstation, and the other type is a stand-alone SCM that is installed and run from a client CWM workstation. Both features are described below.

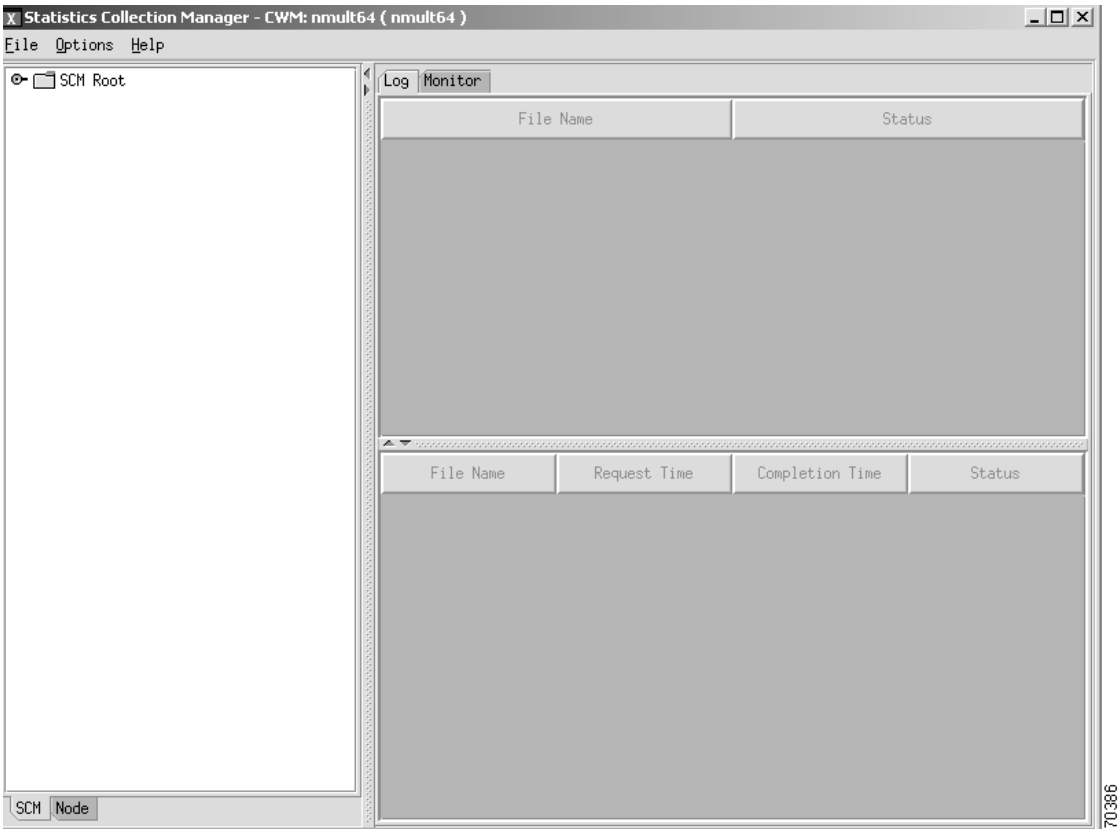
Launching the Statistics Collection Manager

To launch the Statistics Collection Manger application, click on the Statistics Collection Manager icon, which is found on the Network Topology tool bar, or select the Statistics Collection Manager application from the **Apps** pull-down menu located on the main menu bar.

Main Window

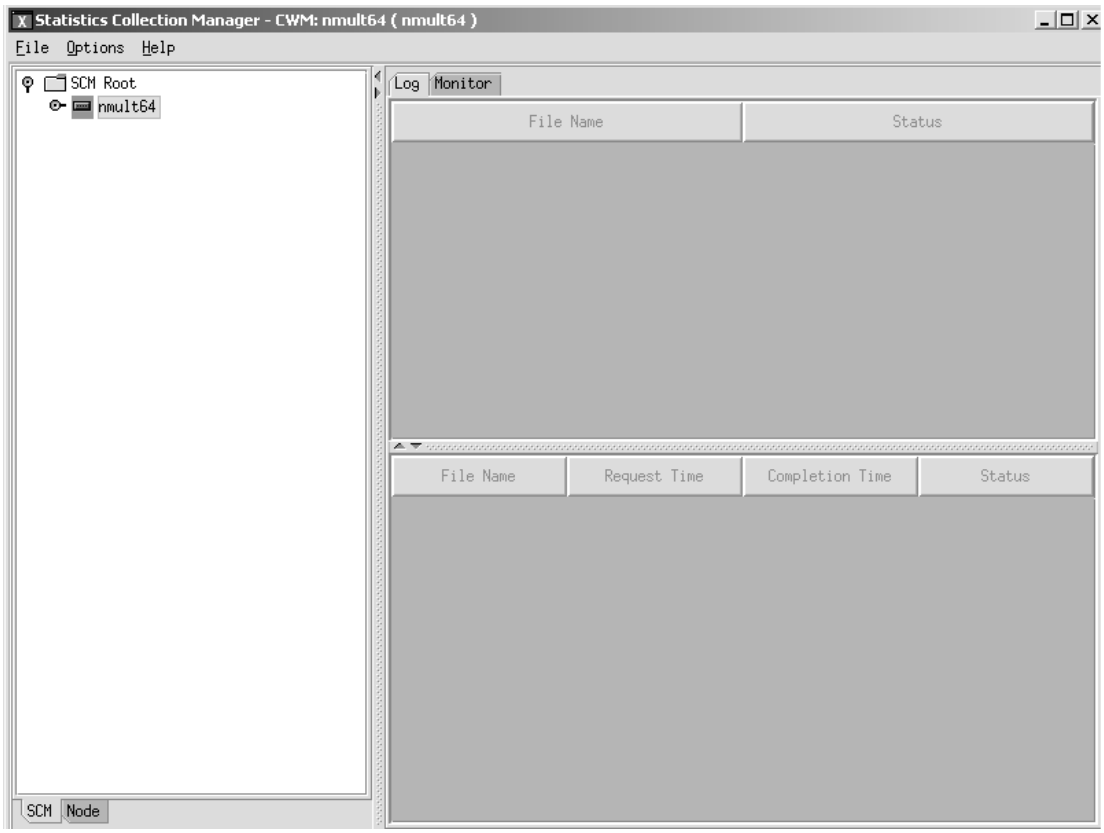
After launching the Statistics Collection Manager application for the first time, you will see a root node called SCM Root in the left panel of the window, as shown in Figure 8-1.

Figure 8-1 Statistics Collection Manager Main Window



Clicking on the eye glass to the left of SCM Root will display the Stats Database Hosts for the SCM Root, as shown in Figure 8-2.

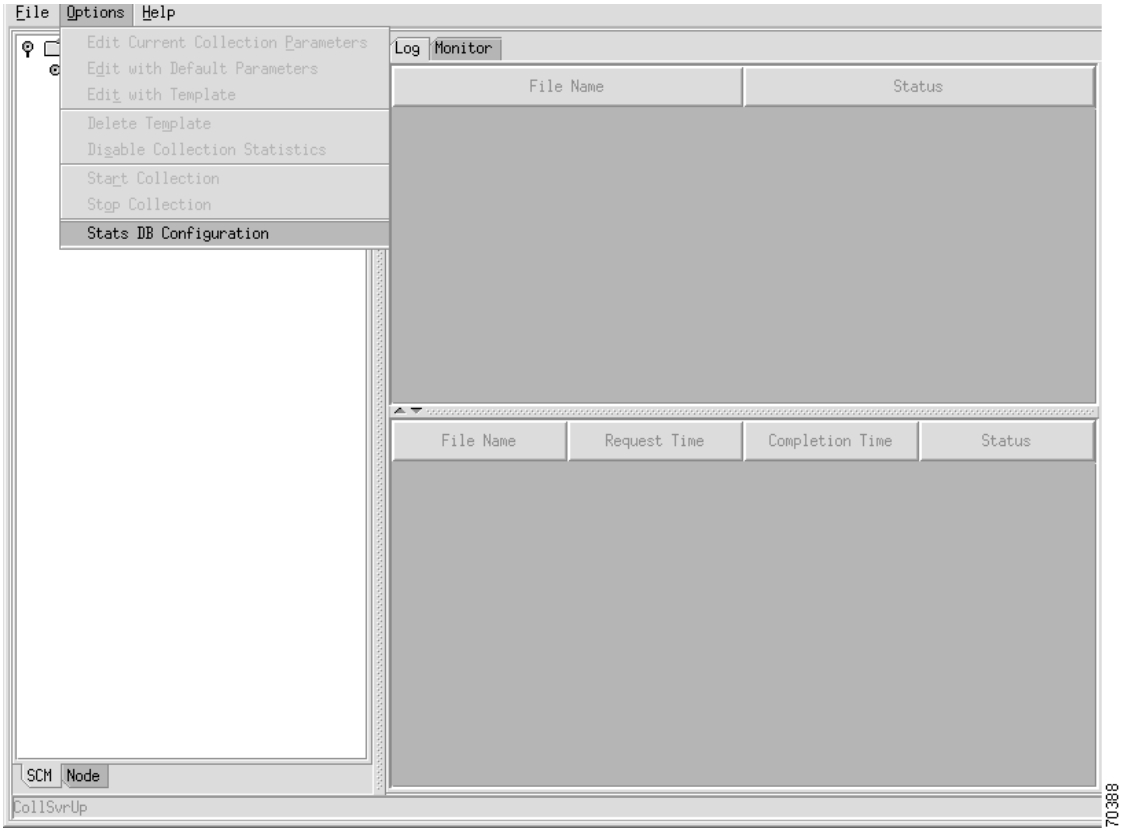
Figure 8-2 Stats Database Hosts



Click on the host to highlight it, and then select the **Options** pull-down menu in order to edit current collection parameters, edit with default parameters, edit with template, delete template, disable collection statistics, start collection, stop collection or configure database stats.

Figure 8-3 shows the **Stats DB Configuration** option selected from the **Options** pull-down menu.

Figure 8-3 Stats DB Configuration Option

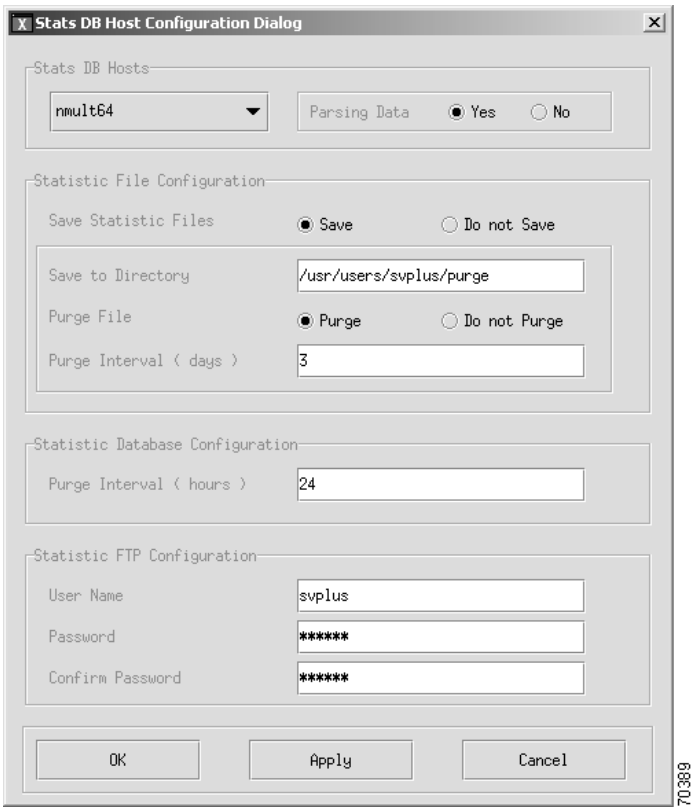


SCM Statistics Database Configuration

After selecting the **Stats DB Configuration** option from the **Options** pull-down menu, the **Stats DB Host Configuration Dialog** appears as shown in Figure 8-4.

When you are finished configuring parameters for the selected **Stats DB Host**, click **Apply** and then **OK**. "Successful Configure" will appear in the lower left hand corner of the SCM main window.

Figure 8-4 Stats DB Host Configuration



Statistic File Configuration

Save Statistic Files Button

This toggle controls the ability to save files as they are parsed from the statistics parser. You set it to **Do not Save** to avoid placing files to the **/usr/users/svplus/purge** directory. Currently, the save directory is not configurable. The default is **Save**.

Save to Directory

You specify the name of the file directory used to store incoming files to be parsed.

Purge File Button

This button controls the ability to purge files as they are parsed from the statistics parser. You set it to **Do not Purge** to avoid deleting files from the **/usr/users/svplus/purge** directory. We recommend you delete old files. The default is **Purge**.

Purge Interval (days)

You specify the value (in days) used to determine which old files are purged from the **/usr/users/svplus/purge** directory when space in your hard disk's Incoming partition drops below twenty megabytes. The files with a date 'N' days older than today's date are purged. (0 = no purging is done.) The default is **3** days.

Statistic Database Configuration

Purge Interval (hours)

You specify the value (in hours) used to determine how long the data is maintained by the CWM database. The default retention period is 24 hours. The maximum retention period is 8784 hours (1 year).

Note If the database contains insufficient space for statistics storage, the statistics collection process may shut down. If this happens, reduce the purge interval to 12 hours.

Statistic FTP Configuration

Username

You specify the FTP username. The default is svplus.

Password

Enter the FTP password. The screen will display asterisks.

Confirm Password

Reenter your FTP password in this field. Once again, the screen will display asterisks.

Launching the SCM Standalone Collector

The Statistics Collection Manager (SCM) for Release 10 of CWM has a new standalone collector that allows a separate SCM collection server in both installation and statistics collection, and is installed and run from a client CWM workstation. This new feature allows you to control and manage statistics collection through a standalone application. The Statistics Controller Server, Statistics Collection Server, and Statistics Parser Server provide statistics applicable to the different cards and nodes.

Note Please refer to Chapter 6 of the CWM Installation Guide for installation procedures for the Standalone SCM.

Launch SCM Standalone Collector through an xterm window by issuing the **SCM** command at the command line. Figure 8-5 shows an xterm window displayed with **SCM** typed at the command line:

Figure 8-5 SCM Stand Alone initialization

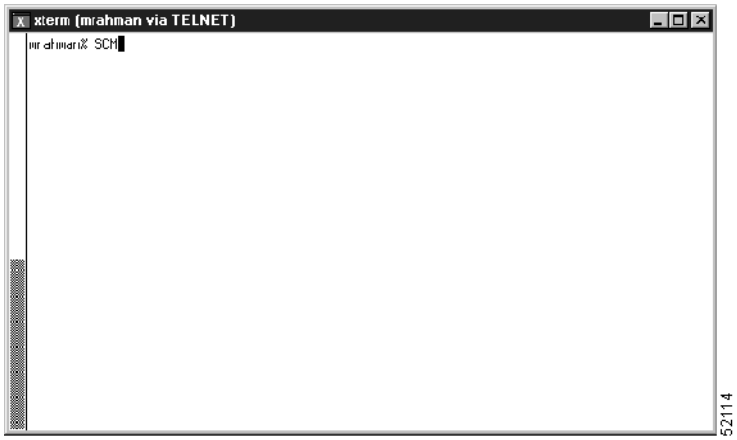
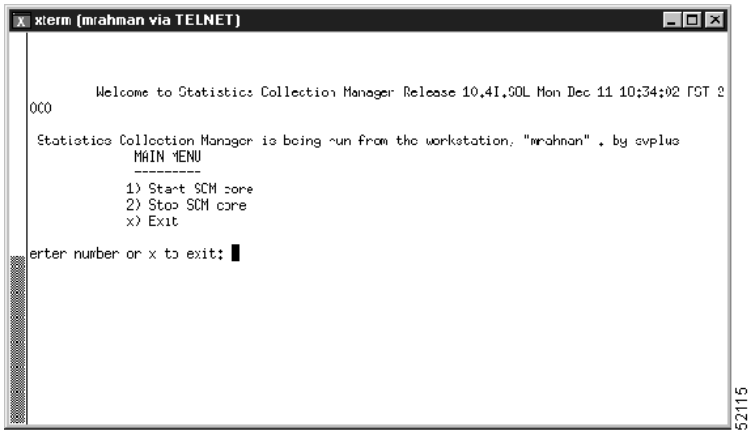


Figure 8-6 shows an xterm window displayed with the SCM main menu options:

Figure 8-6 SCM start core, stop core, and exit options

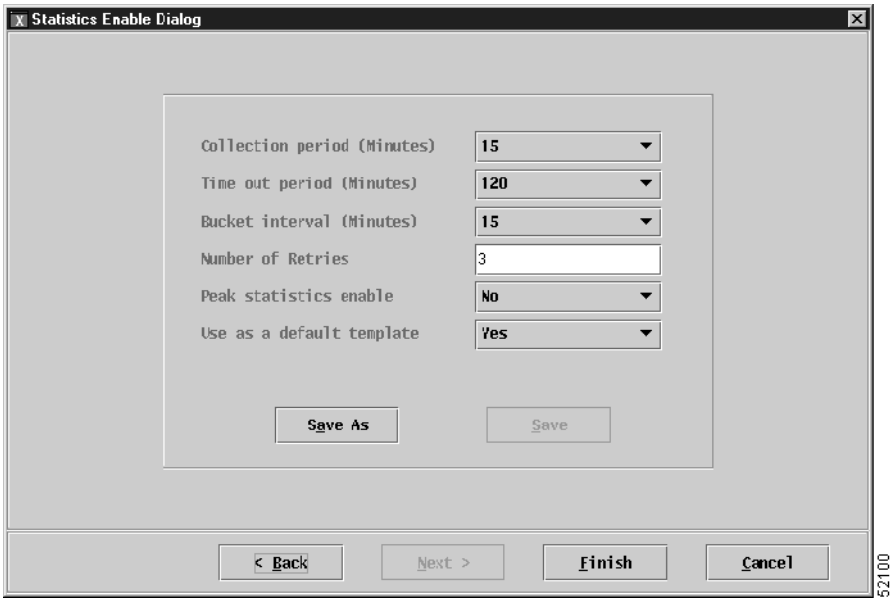


SCM Statistics Enable

Figure 8-7 shows the Statistics Enable dialog box which appears after you start the SCM core. This window allows you to set the collection period in minutes, the time out period in minutes, the bucket interval in minutes, the number of retries, and the peak statistics enable. The last drop-down in this dialog box asks whether you would like to use your selected settings as a default template. The switch implements these selected values and sends confirmation back to the SCM Controller Server.

Note Statistics Enable is only accepted from the CWM machine which is registered as Statistics Master on the nodes. (It can be set via telnet to BPX, IGX and IPX nodes by using the **cnfstatmast** command; the **cnfstatsmgr** command must be used for MGX-8220 and MGX-8250/8230/8850-R1.

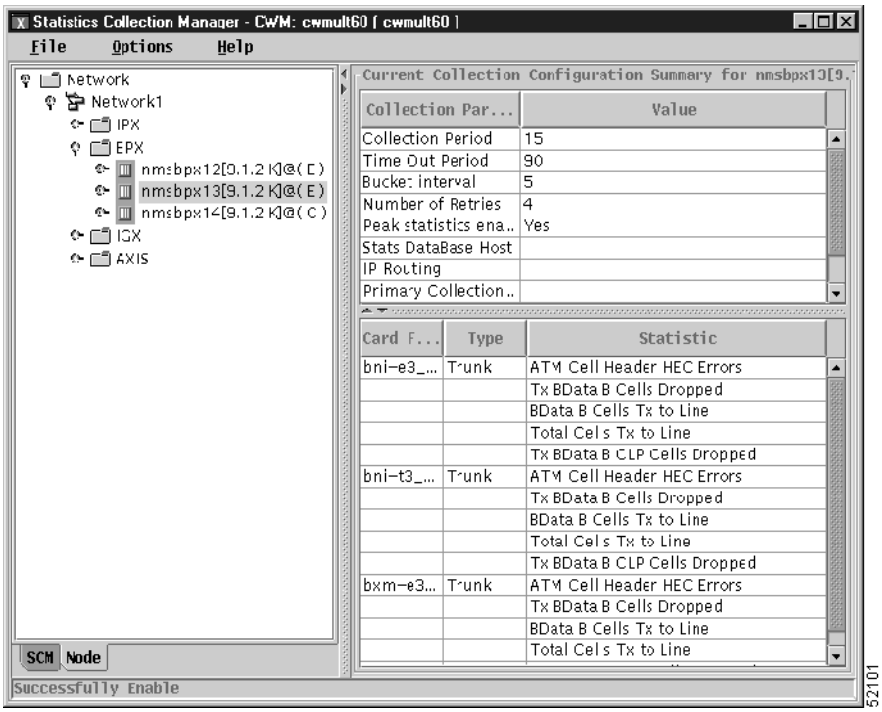
Figure 8-7 Statistics Enable Dialog



SCM Statistics Update

Figure 8-8 shows the Update Stats enabling information window which appears after the parameters in the Statistics Enable dialog box have been set.

Figure 8-8 Update Stats enabling information



SCM Statistics Disable

Figure 8-9 shows the **Disable Collection Statistics** option, and Figure 8-10 shows Statistics Disabling completed.

Figure 8-9 Disabling Stats

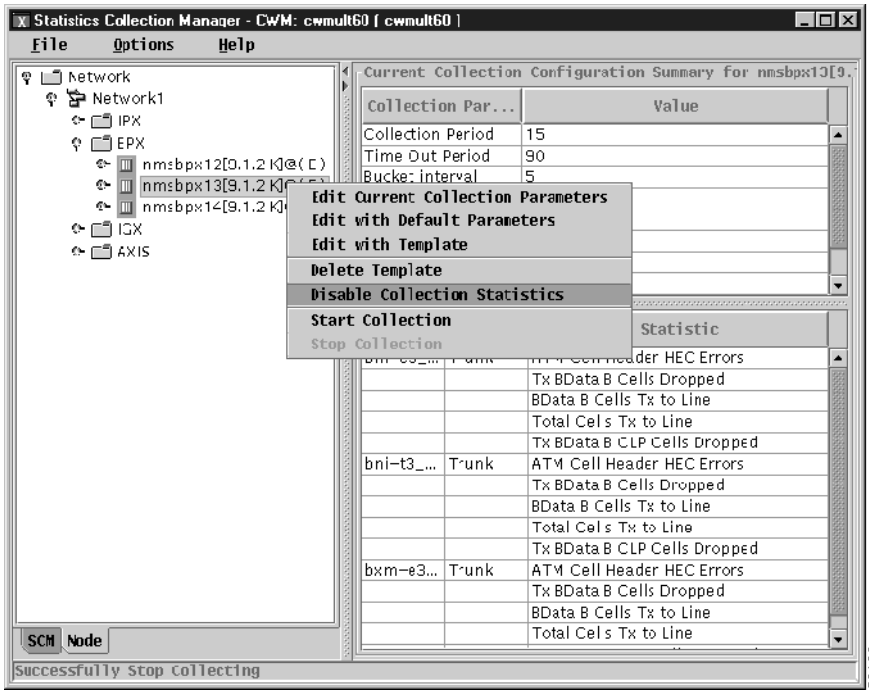
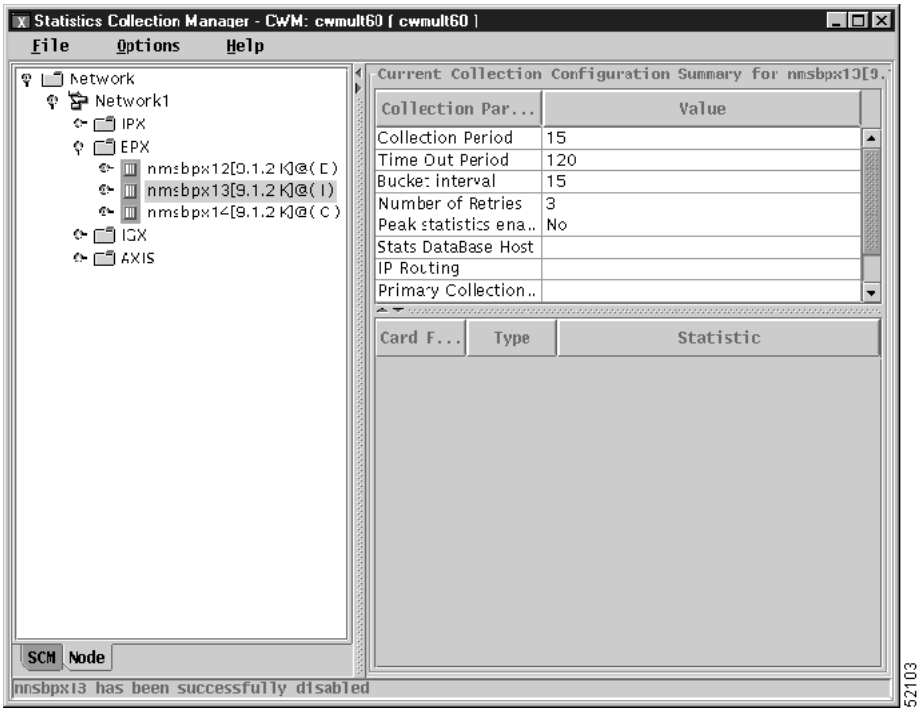


Figure 8-10 Statistics Disabling complete



SCM Statistics Collection

Figure 8-11 shows the **Start Statistics Collection** option. Figure 8-12 shows the **Statistics Collection configuration** dialog box which appears after the **Start Statistics Collection** option has been selected.

Figure 8-11 Start Statistics Collection

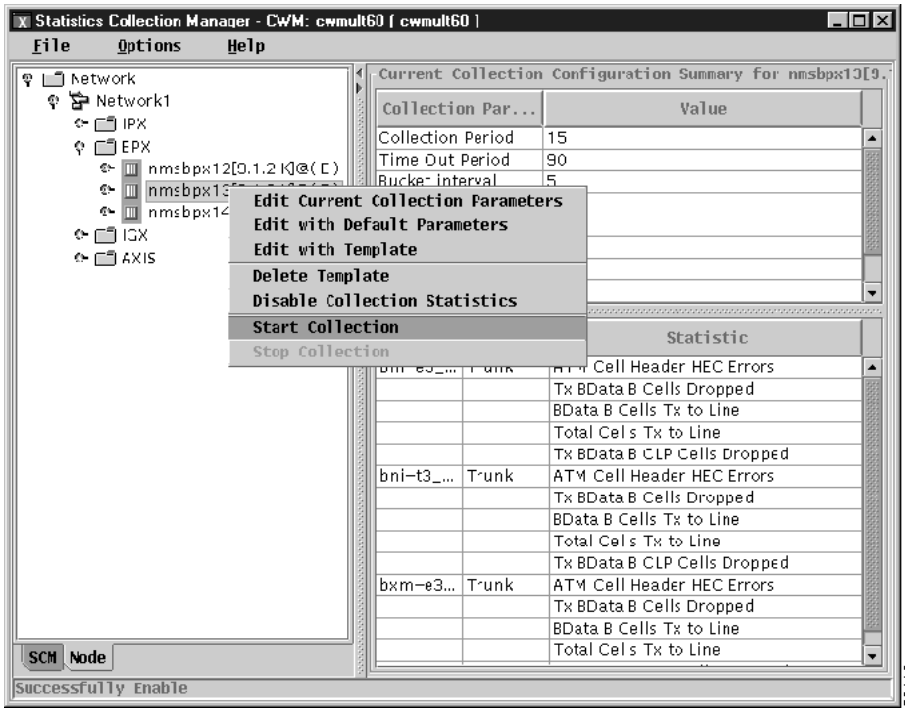


Figure 8-12 Statistics Collection configuration

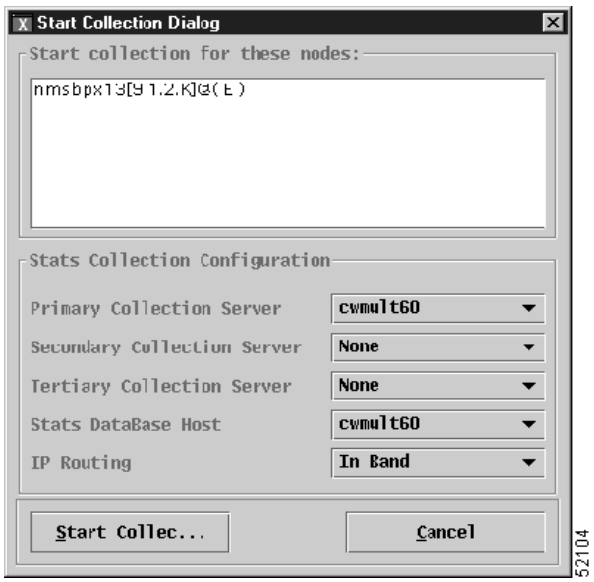


Figure 8-13 shows the **Statistics Collection** started, with collection parameters, values and statistics populating the appropriate data fields in the right panel of the SCM main window.

Figure 8-13 Statistics Collection started

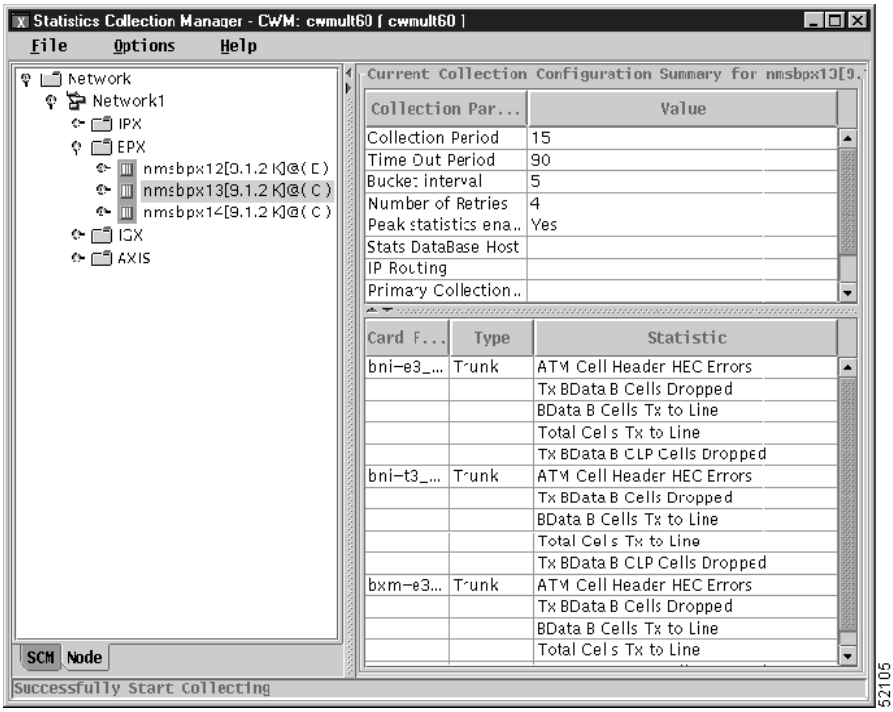


Figure 8-14 displays pending and completed stats file information, and Figure 8-15 displays stats file summary information

Figure 8-14 .Pending and completed stats files information

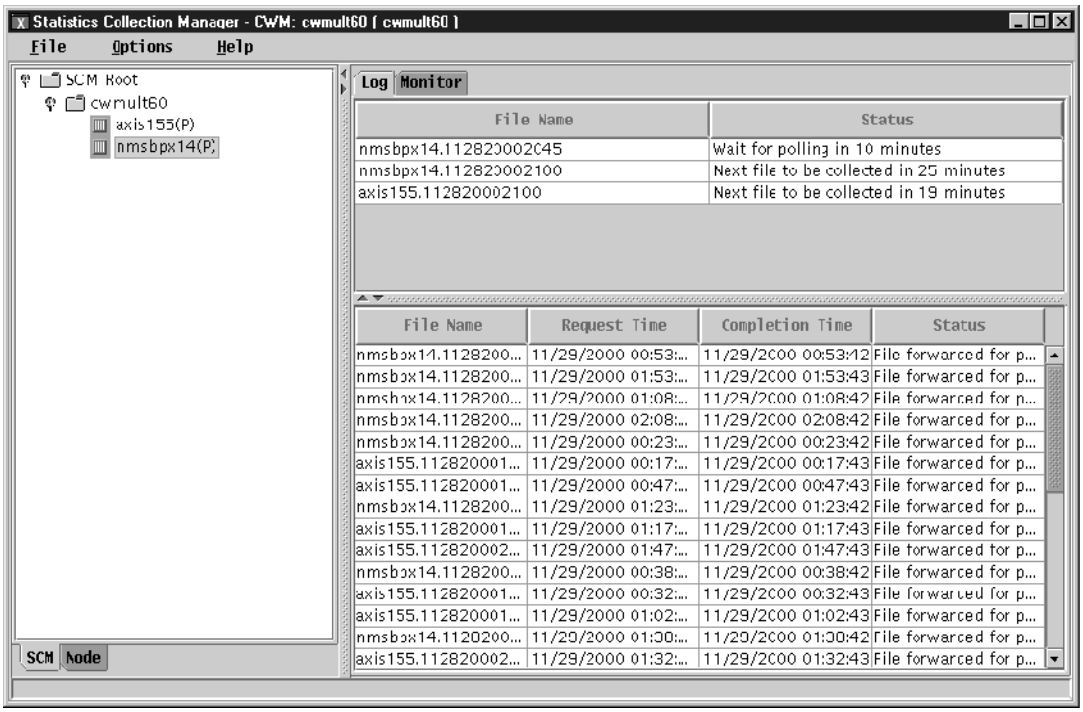
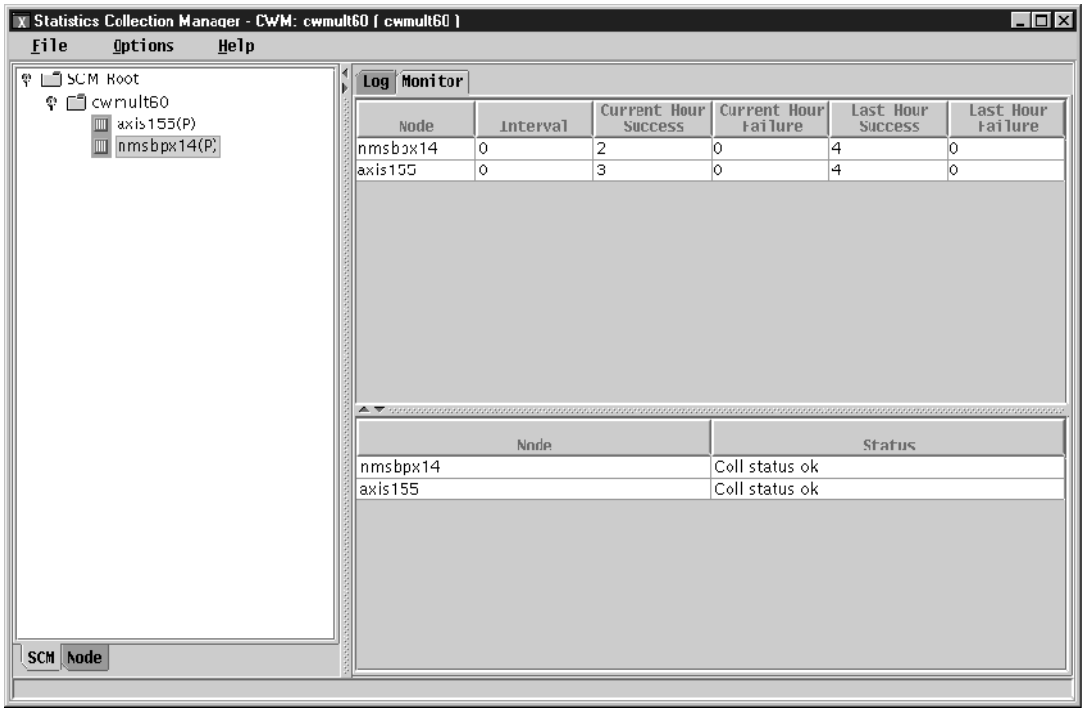


Figure 8-15 Stats File summary information



Stop Statistics Collection

Figure 8-16 shows the **Stop Collection** option. After selecting the **Stop Collection** option from the **Options** pull-down menu, the Stop Collection dialog box appears as shown in Figure 8-17.

Figure 8-16 Stop Stats collection

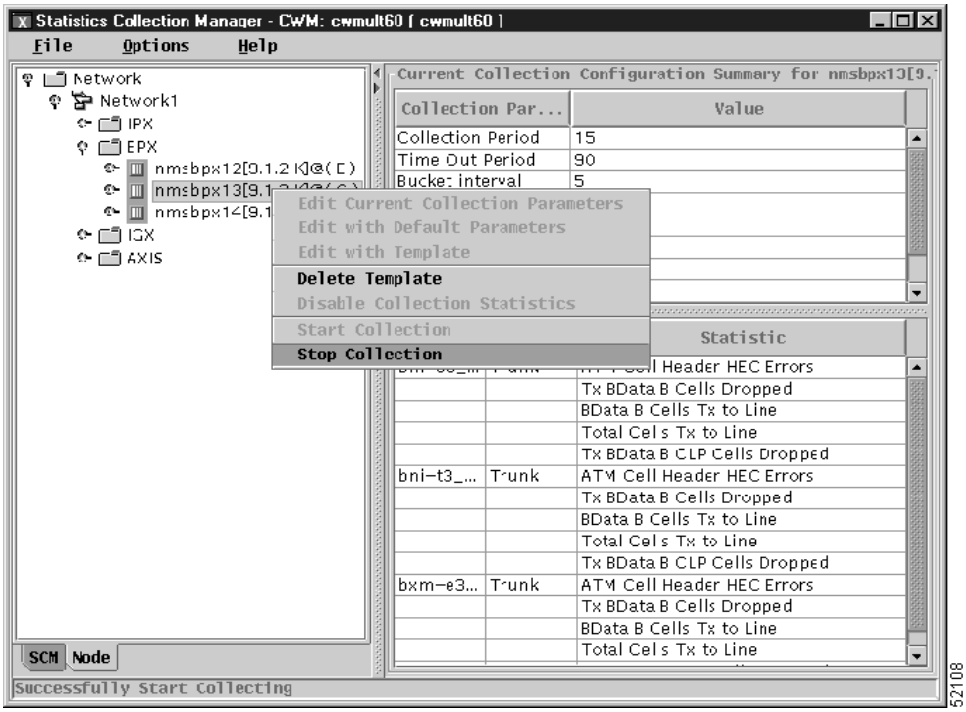
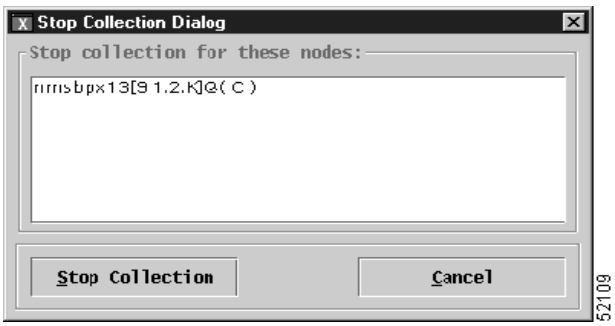


Figure 8-17 Stop Stats collection confirmation



SCM Primary/Secondary/Tertiary

SCM Primary/Secondary/Tertiary GUIs provide distributed collection and statistics collection redundancy. SCM redundancy means that the secondary and tertiary SCM collection servers still continue to collect statistics when the primary SCM collection server is not reachable or completely shut down. Distributed collection means that you can distribute statistics collection from all switch nodes to different SCM collection servers. For example, if the connection to the Primary SCM is shut down for any reason, whether the FTP or TFTP connection has been disrupted, or if the Primary SCM shuts down, then the Secondary SCM can take over the statistics collection processes. If the Secondary SCM shuts down for any reason, the Tertiary SCM can take over the statistics collection processes.

P/S/T is always dependant upon the assignment of the collection server. You can use the **cnfcollsvr** command to redirect collectors to a CWM host.

The Start Collection Dialog allows collection configuration for the Primary, Secondary, and Tertiary collection servers. Also, the stats database host can be set, and IP Routing can be designated as inband or out-of-band as seen in Figure 8-12.

CWM-CWM Communications

Release 10 of Cisco WAN Manager has been designed to enable multiple CWM workstations to manage a network with improved network synchronization and scalability. The architecture uses a server-client structure for communications between the CWM server and client processes.

CWM workstations use CWM-CWM Communications to synchronize user data with each other. When user data is provisioned or changed, the CWM workstations will propagate the new data to the other CWM workstations. The user is able to continue the provisioning of network data, even when communications between a Primary CWM and Secondary CWM have been interrupted. If for any reason the communications between CWM servers are interrupted, the provisioning of the user data will be suspended on the Secondary CWM, but not on the Primary CWM as user data provisioning will continue on the Primary CWM. During that time, the provisioning of user data and monitoring of the network are not impacted.

In a given wide area network managed by Release 10 of CWM, the first CWM workstation to begin operation will assume the role of Primary CWM. As other CWM workstations become active, they will take on Secondary CWM workstation roles. The only difference in function between Primary and Secondary CWM workstations is that the Primary CWM workstation would provide the Secondary CWM workstations with user data when the Secondary CWM workstation launches.

Priority numbers of all Secondaries are assigned by the Primary at the time a Secondary registers with the Primary. It is based on “first-come-first-serve” logic. All the Secondaries have the same privilege except that the Secondary with priority 1 will take over as the Primary if the Primary shuts down.

SCM CWM-CWM Gateway Support

Stats collection is populated from the Primary SCM to the Secondary SCM. Primary gateways save enabling information and forward data to the Secondary host via the Stats Master.

Time Sync

Timing in SCM is qualified by the node time and a sequence to connect from Primary to Secondary with a set maximum amount of retries.

SCM Inband and Out-of-band

TFTP and FTP are used to transfer files using the network IP address for inband communications, and the LAN IP address for out-of-band communications.

SCM Dual Collectors for Legacy Nodes

Dual collectors for Legacy Nodes include the following: BPX, IPX, IGX, Axis, MGX 8850 Release 1; single collector for MGX 8850 Release 2.

SES Nodes include MGX 8850 Release 2, and BPX/SES.

SCM History Files Collection

The default for History Files Collection in stand alone SCM is No History Files Collection. History Files collection can be set from one to a maximum of three files for collection.

Group Nodes by Platform

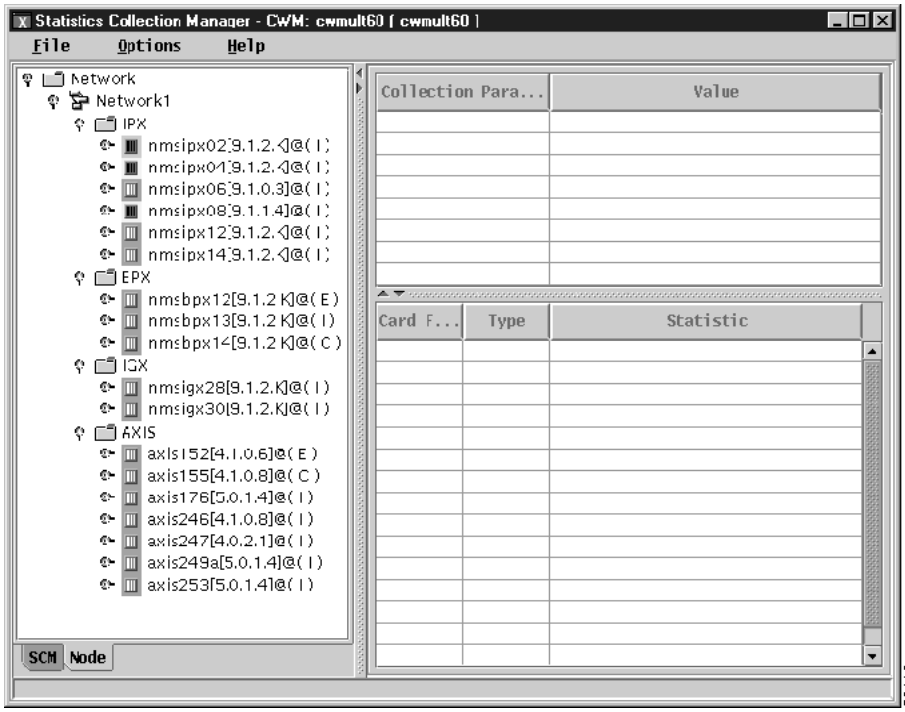
Node View

The node view provides a hierarchical view of network elements. The node panel enables you to do the following operations:

- Select a node in the navigator panel to edit collection parameters or to begin or end statistics collection
- Select a specific node or element to configure statistics collection
- Display the statistics collection parameters after selecting a node
- Select multiple nodes to start, stop, or enable collection

Figure 8-18 shows nodes grouped by platform.

Figure 8-18 Nodes grouped by platform



Window Refresh

SCM provides a refresh option that displays all changes made to node configurations. To refresh the SCM window you must collapse the expanded SCM tree, as shown in Figure 8-18, by double clicking on the root node, and then re-expanding the tree to see the new configuration. This refresh option applies to Primary, Secondary, and Tertiary configurations.

Card Families

The following is a list of card families mapped to the cards they support. The list is organized by platform, with card families and the card(s) it supports listed after each platform.

IPX switch:

- ait_91
  - AIT
- cdp_91
  - CDP
- sdp_91
  - SDP
  - LDP
- fastpad_91
  - FTC

- uxm_91
  - UXM
- uxm_92
  - UXM
- uxm_93
  - UXM
- frp_91
  - FRP
- ntc_91
  - NTC

IGX switch:

- btm_91
  - BTM
  - ALM-A
  - ALM-B
- cdp_91
  - CDP
  - UVM
- sdp_91
  - SDP
  - LDP
- fastpad_91
  - FTC
- uxm_91
  - UXM
- uxm_92
  - UXM
- uxm_93
  - UXM
- urm_93
  - URM
- frp_91
  - FRP
  - UFM
  - UFM-U
- ntc_91
  - NTC

BPX switch:

- asi-t3_91
  - ASI_T3_2
  - ASI0_E3
  - ASI0_T3
- asi-e3_91
  - ASI_E3_2
- asi-oc3_91
  - ASI_OC3
- asi-t3_92
  - ASI_T3_2
  - ASI0_E3
  - ASI0_T3
- asi-e3_92
  - ASI_E3_2
- asi-oc3_92
  - ASI_OC3
- asi-t3_93
  - ASI_T3_2
  - ASI0_E3
  - ASI0_T3
- asi-e3_93
  - ASI_E3_2
- asi-oc3_93
  - ASI_OC3
- bxm_t3_91
  - BXM_T3_8_SMF
  - BXM_T3_8_MMF
  - BXM_T3_8_SMFLR
  - BXM_T3_8_SNM
  - BXM_T3_12_SMF
  - BXM_T3_12_MMF
  - BXM_T3_12_SMFLR
  - BXM_T3_12_SNM
- bxm_t3_92
  - BXM_T3_8_SMF
  - BXM_T3_8_MMF
  - BXM_T3_8_SMFLR
  - BXM_T3_8_SNM

  - BXM_T3_12_SMF
  - BXM_T3_12_MMF
  - BXM_T3_12_SMFLR
  - BXM_T3_12_SNM
- bxme_t3_92
  - BXM_T3_12 (Enhanced)
- bxm_t3_93
  - BXM_T3_8_SMF
  - BXM_T3_8_MMF
  - BXM_T3_8_SMFLR
  - BXM_T3_8_SNM
  - BXM_T3_12_SMF
  - BXM_T3_12_MMF
  - BXM_T3_12_SMFLR
  - BXM_T3_12_SNM
- bxme_t3_93
  - BXM_T3_12 (Enhanced)
- bxm_e3_91
  - BXM_E3_8_SMF
  - BXM_E3_8_MMF
  - BXM_E3_8_SMFLR
  - BXM_E3_8_SNM
  - BXM_E3_12_SMF
  - BXM_E3_12_MMF
  - BXM_E3_12_SMFLR
  - BXM_E3_12_SNM
- bxm_e3_92
  - BXM_E3_8_SMF
  - BXM_E3_8_MMF
  - BXM_E3_8_SMFLR
  - BXM_E3_8_SNM
  - BXM_E3_12_SMF
  - BXM_E3_12_MMF
  - BXM_E3_12_SMFLR
  - BXM_E3_12_SNM
- bxme_e3_92
  - BXM_E3_12 (Enhanced)
- bxm_e3_93

  - BXM_E3_8_SMF
  - BXM_E3_8_MMF
  - BXM_E3_8_SMFLR
  - BXM_E3_8_SNM
  - BXM_E3_12_SMF
  - BXM_E3_12_MMF
  - BXM_E3_12_SMFLR
  - BXM_E3_12_SNM
- bxme_e3_93
  - BXM_E3_12 (Enhanced)
- bxm_oc3_91
  - BXM_OC3_4_SMF
  - BXM_OC3_4_MMF
  - BXM_OC3_4_SMFLR
  - BXM_OC3_4_SNM
  - BXM_OC3_8_SMF
  - BXM_OC3_8_MMF
  - BXM_OC3_8_SMFLR
  - BXM_OC3_8_SNM
  - BXM_OC3_4_STM1E
  - BXM_OC3_8_STM1E
  - BXM_OC3_4_XLR
  - BXM_OC3_8_XLR
  - BPX_MNCH
- bxm_oc3_92
  - BXM_OC3_4_SMF
  - BXM_OC3_4_MMF
  - BXM_OC3_4_SMFLR
  - BXM_OC3_4_SNM
  - BXM_OC3_8_SMF
  - BXM_OC3_8_MMF
  - BXM_OC3_8_SMFLR
  - BXM_OC3_8_SNM
  - BXM_OC3_4_STM1E
  - BXM_OC3_8_STM1E
  - BXM_OC3_4_XLR
  - BXM_OC3_8_XLR
  - BPX_MNCH

- bxm_oc3_93
  - BXM_OC3_4_SMF
  - BXM_OC3_4_MMF
  - BXM_OC3_4_SMFLR
  - BXM_OC3_4_SNM
  - BXM_OC3_8_SMF
  - BXM_OC3_8_MMF
  - BXM_OC3_8_SMFLR
  - BXM_OC3_8_SNM
  - BXM_OC3_4_STM1E
  - BXM_OC3_8_STM1E
  - BXM_OC3_4_XLR
  - BXM_OC3_8_XLR
  - BPX_MNCH
- bxm_oc12_91
  - BXM_OC12_1_SMF
  - BXM_OC12_1_MMF
  - BXM_OC12_1_SMFLR
  - BXM_OC12_1_SNM
  - BXM_OC12_2_SMF
  - BXM_OC12_2_MMF
  - BXM_OC12_2_SMFLR
  - BXM_OC12_2_SNM
  - BME_OC12_1_SMF
  - BME_OC12_1_MMF
  - BME_OC12_1_SMFLR
  - BME_OC12_1_SNM
  - BME_OC12_2_SMF
  - BME_OC12_2_MMF
  - BME_OC12_2_SMFLR
  - BME_OC12_2_SNM
  - BXM_OC12_1_XLR
  - BXM_OC12_2_XLR
- bxm_oc12_92
  - BXM_OC12_1_SMF
  - BXM_OC12_1_MMF
  - BXM_OC12_1_SMFLR
  - BXM_OC12_1_SNM

  - BXM_OC12_2_SMF
  - BXM_OC12_2_MMF
  - BXM_OC12_2_SMFLR
  - BXM_OC12_2_SNM
  - BME_OC12_1_SMF
  - BME_OC12_1_MMF
  - BME_OC12_1_SMFLR
  - BME_OC12_1_SNM
  - BME_OC12_2_SMF
  - BME_OC12_2_MMF
  - BME_OC12_2_SMFLR
  - BME_OC12_2_SNM
  - BXM_OC12_1_XLR
  - BXM_OC12_2_XLR
- bxm_oc12_93
  - BXM_OC12_1_SMF
  - BXM_OC12_1_MMF
  - BXM_OC12_1_SMFLR
  - BXM_OC12_1_SNM
  - BXM_OC12_2_SMF
  - BXM_OC12_2_MMF
  - BXM_OC12_2_SMFLR
  - BXM_OC12_2_SNM
  - BME_OC12_1_SMF
  - BME_OC12_1_MMF
  - BME_OC12_1_SMFLR
  - BME_OC12_1_SNM
  - BME_OC12_2_SMF
  - BME_OC12_2_MMF
  - BME_OC12_2_SMFLR
  - BME_OC12_2_SNM
  - BXM_OC12_1_XLR
  - BXM_OC12_2_XLR
- bxme_oc3_92(Enhanced Cards)
  - BXM_OC3_4_SMF
  - BXM_OC3_4_MMF
  - BXM_OC3_4_SMFLR
  - BXM_OC3_8_SMF

  - BXM_OC3_8_MMF
  - BXM_OC3_8_SMFLR
  - BXM_OC3_4_STM1E
  - BXM_OC3_8_STM1E
  - BXM_OC3_4_XLR
  - BXM_OC3_8_XLR
- bxme_oc3_93(Enhanced Cards)
  - BXM_OC3_4_SMF
  - BXM_OC3_4_MMF
  - BXM_OC3_4_SMFLR
  - BXM_OC3_8_SMF
  - BXM_OC3_8_MMF
  - BXM_OC3_8_SMFLR
  - BXM_OC3_4_STM1E
  - BXM_OC3_8_STM1E
  - BXM_OC3_4_XLR
  - BXM_OC3_8_XLR
  - BXM_OC12_1_SMF
- bxme_oc12_92(Enhanced Cards)
  - BXM_OC12_1_MMF
  - BXM_OC12_1_SMFLR
  - BXM_OC12_2_SMF
  - BXM_OC12_2_MMF
  - BXM_OC12_2_SMFLR
  - BME_OC12_1_SMF
  - BME_OC12_2_SMF
  - BME_OC12_2_SMFLR
  - BME_OC12_2_SNM
  - BXM_OC12_1_XLR
  - BXM_OC12_2_XLR
- bxme_oc12_93(Enhanced Cards)
  - BXM_OC12_1_MMF
  - BXM_OC12_1_SMFLR
  - BXM_OC12_2_SMF
  - BXM_OC12_2_MMF
  - BXM_OC12_2_SMFLR
  - BME_OC12_1_SMF
  - BME_OC12_2_SMF

  - BME_OC12_2_SMFLR
  - BME_OC12_2_SNM
  - BXM_OC12_1_XLR
  - BXM_OC12_2_XLR
- bni-t3_91
  - BNI_T3
- bni-t3_92
  - BNI_T3
- bni-t3_93
  - BNI_T3
- bni-e3_91
  - BNI_E3
- bni-e3_92
  - BNI_E3
- bni-e3_93
  - BNI_E3
- bni-oc3_91
  - BNI_OC3
- bni-oc3_92
  - BNI_OC3
- bni-oc3_93
  - BNI_OC3

AXIS:

- frsm_40
  - FRSM_4T1
  - FRSM_4E1
  - FRSM_4T1_C
  - FRSM_4E1_C
  - FRSM_HS1
  - FRSM_HS1_B
  - FRSM_8T1
  - FRSM_8E1
  - FRSM_2CT3
  - FRSM_2T3
  - FRSM_2E3
  - FRSM_2HS2
- ausm_40
  - AUSM_4T1

  - AUSM_4E1
  - AUSM_8T1
  - AUSM_8E1
  - AUSM_B_8T1
  - AUSM_B_8E1
- cesm_40
  - CESM_4T1
  - CESM_4E1
  - CESM_8T1
  - CESM_8E1
  - CESM_T3
  - CESM_E3
- bnm-t3_40
  - BNM_T3
- bnm-e3_40
  - BNM_E3
- bnm-155_40
  - BNM_155

POPEYE Release 1:

- frsm_40
  - FRSM_4T1
  - FRSM_4E1
  - FRSM_4T1_C
  - FRSM_4E1_C
  - FRSM_HS1
  - FRSM_HS1_B
  - FRSM_8T1
  - FRSM_8E1
  - FRSM_2CT3
  - FRSM_2T3
  - FRSM_2E3
  - FRSM_2HS2
- ausm_40
  - AUSM_4T1
  - AUSM_4E1
  - AUSM_8T1
  - AUSM_8E1
  - AUSM_B_8T1

  - AUSM_B_8E1
- cesm_40
  - CESM_4T1
  - CESM_4E1
  - CESM_8T1
  - CESM_8E1
  - CESM_T3
  - CESM_E3
- pxm_1_40
  - PXM_1
  - PXM_OC3
  - PXM_OC12
  - PXM_T3E3
- srm-t3_92
  - SRM_3T3
  - SRME
- srm-SONET_92
  - SRME_1OC3
  - SRME_1STS3

POPEYE II:

- axsmt3e3_50
  - AXSM16_T3E3
  - AXSM16_T3E3_B(AXSM B)
- axsmoc3-12_50
  - AXSM8_OC3
  - AXSM16_OC3
  - AXSM16_OC3_B(axsm B)
  - AXSM4_OC12
  - AXSM4_OC12_B(axsm B)
- axsmoc48_50
  - AXSM1_OC48
  - AXSM1_OC48_B(axsm B)
- axsmet3e3_50
  - AXSM16_T3E3_E
- axsmeoc3-12_50
  - AXSM8_OC3_E
  - AXSM2_OC12_E
  - AXSM8_STM1_E

Configuring Statistics Collection

After parameters have been set, right click to choose one of the following options:

- Edit Current Collection Parameters—Allows current collection parameters to be edited.
- Edit with Default Parameters—Allows current collection parameters to be edited with default parameters.
- Edit with Template—Allows editing with template.
- Delete Template—Allows you to delete a template.
- Disable Collection Statistics—Allows you to disable collection statistics.
- Start Collection—Tells the Statistics Manager to begin collecting statistics from the selected nodes, if the node has statistics enabled.
- Stop Collection—Tells the Statistics Manger to stop collecting from the selected nodes, if statistics are already being collected.
- Stats DB Host Configuration—Sets statistics parameters for the File and Database, including Save Statistics Files, Purge File, and Purge Interval.

Note The Start Collection option is not enabled unless statistics have been enabled for a network element.

Table 8-1 Statistics Collection Parameters (modifiable)

Parameter	Description
Collection Period	Specify the interval value (in minutes) where statistics are gathered from the network. The collection period refers to the time it takes to create a stats file. The file will include multiple buckets. The default is 15 minutes.
Time-Out Period	Specify the time-out value (in minutes for TFTP GET requests. Increase this value on busy networks. Busy networks should be configured for a high value. The default is 120 minutes.
Bucket Interval	Specify the Bucket Interval Period value (in minutes) to be kept for the single bucket on the node. The default is 15 minutes.
Number of Retries	Specify the number of retries the child process makes in attempting to get files from the network. The default is 3 retries.

Table 8-1 Statistics Collection Parameters (modifiable)

Parameter	Description
Peak Statistics Enable	Specify peak statistics values on network by selecting No or Yes. The peak value represents the maximum value of buckets. The default is No.
Use as a default template	You have the option to use this as a default template by selecting No or Yes. Yes is the default.

How Statistics are Used

Statistics are used to show network performance. Raw data can be used for monitoring nodes in your network, and for customer billing purposes. The Wingz Reports application provides statistics collection reporting.

Summary Report and Wingz Report

This chapter describes the Summary Report application and the Wingz Report application.

Overview of Summary Reports and Wingz Reports

The CWM Summary Report application is designed to provide easy access to basic performance reports. Once you select the report type, object instance, and plot duration, the report data is retrieved from the CWM Statistics Collection Manager (SCM), and is plotted within the respective Report Application window.

The Performance Data reports are based on historical statistics collected by the CWM SCM. To generate a report, you must select the appropriate statistic type. No restrictions exist on the bucket interval setting for Summary Reports. When the bucket interval changes within the report plot period, the Summary Report application makes an adjustment to normalize the data according to the plot interval. The CWM Summary Report application issues an error when a bucket interval change is detected within the plot period.

Note Restrictions exist on the bucket interval setting for Wingz Reports. The bucket interval must match the bucket interval set in SCM.

The following CWM Summary Reports are available:

- Resource Capacity
  - Network Report
  - Top Utilization Report
- Performance Data
  - Connection

    Connection Traffic Summary

    Connection Traffic Dropped Summary (not currently supported for CESM)
  - Trunk

    Trunk Traffic Summary
  - Port

    Port Traffic Summary

Launching WingZ Reports

The current Wingz based Report application provides a very complex and flexible interface that allows you to select and manipulate a large number of statistic types.

To launch Wingz reports, complete the following procedure:

Step 1 Open a terminal window.

Step 2 Enter the **runwingz** command at the prompt.

Note If you enter an uppercase w, for example, **Wingz**, the **Statistics** button will not be displayed on the Wingz toolbar.

Entering the **runwingz** command at the prompt displays the CWM Statistics window, shown in Figure 9-1, "CWM Statistics Window".

Figure 9-1 CWM Statistics Window

This application provides access to your network statistics stored in the Informix OnLine database via the **Statistics** menu in the CWM Statistics window. The **Statistics** menu provides options to display data reports, edit object linkage, and deactivate statistics generation on non-existent nodes.

Statistics Menu

You select this menu to access the following menu options:

Raw Data Report Option

You select this option to filter the graphical reports of data according to the choices provided in the menu.

Remove non-active Node Option

You select this option to remove statistics for nodes no longer in use.

Initialize Option

You select this option to reset the **Statistics** pull-down windows.

Note Timestamps on the statistics buckets collected by CWM are synchronized with network time.

Raw Data Reports

The **Raw Data Report** option displays the Raw Data Report window. This window provides options allowing you to enable customization of your reports. You select this option to generate reports for Connections, Service Lines, Trunks, and Ports. Once you select one of these object types in the Raw Data Report form, associated parameter fields are displayed.

You use the same procedure to configure all types of Raw Data Reports.

Figure 9-2 Raw Data Report Window

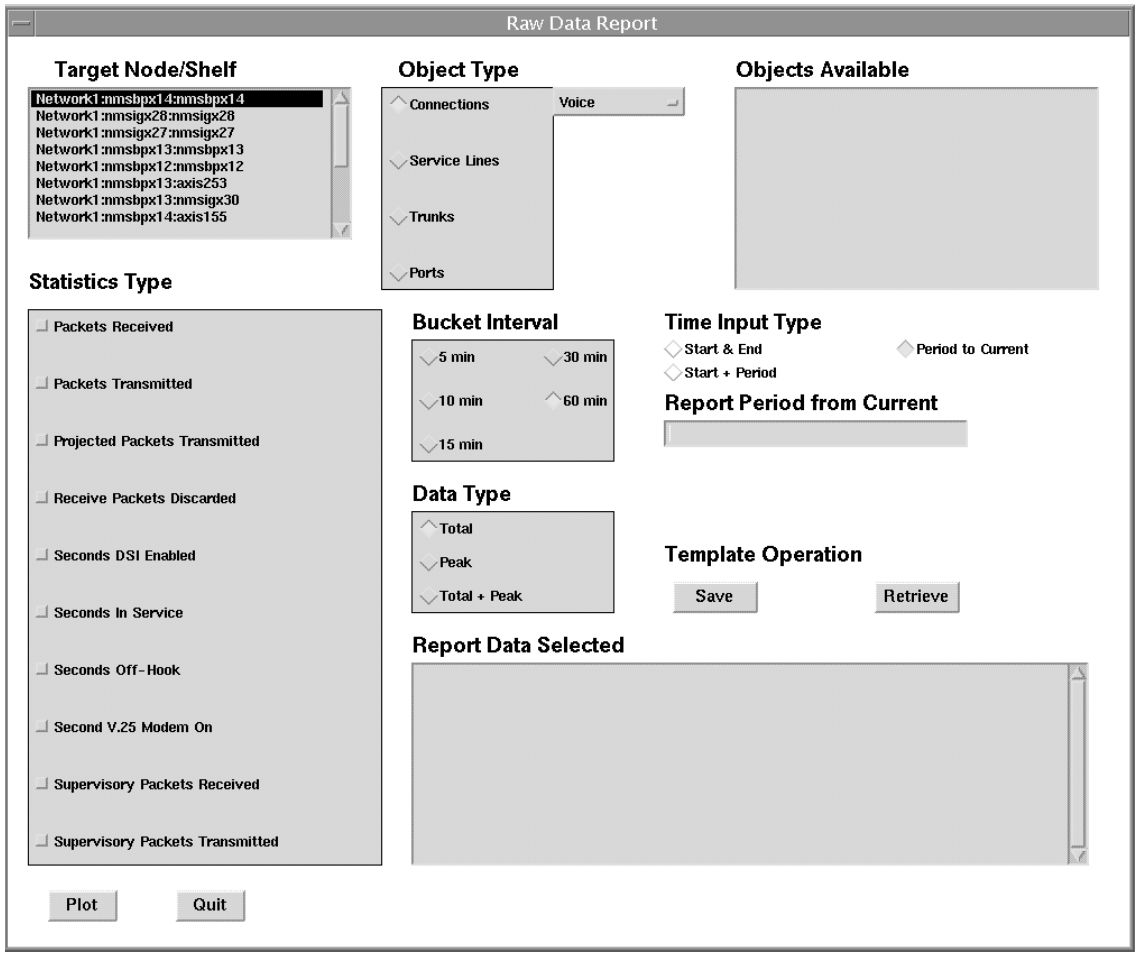


Table 9-1 Time Input Type

Time Input Type	Description
Start & End	Use this parameter to define statistics spanning a starting date and time, to an ending date and time.
Start + Period	Use this parameter to define statistics beginning at a starting date and time, and spanning a specified period or minutes (m), days (d), and/or hours (h). Example: To indicate a single value for one day and two hours and 10 minutes, type: *1d 2h 10m*
Period to Current (default)	Use this parameter to define statistics from the present backwards, with values of minutes (m), hours (h), or days (d). Type the number of m, h, or d into the Report Period field. Example: To indicate a value for 24 hours, type: *24h*

1. After you define a time value, select an object name in the Objects Available field. This results in the display of the selected statistics in the Report Data field.
2. Click on the **Plot** button to start the query. A Querying database window is displayed for each statistic retrieved during the search process. When no statistics are found, the "No data available" message is displayed. When statistics are enabled and collected, a Select Graph Type window is displayed.

A displayed Raw Data Report can be printed selecting the **Page Preview** or **Print** option in the **File** menu on the Wingz menu bar (titled CWM Statistics).

Remove Non-Active Nodes

Select this option from the **Statistics** menu to display the **Remove Node** menu. In the **Target Node** pane, select the nodes you want to delete, then click on the **Apply** button. When no non-active nodes exist, a "No non-active node is defined in the database" message is displayed.

Initialize

Select this option to reset the Statistics window.

Delete Statistical Records

Use the **delstrecs** function to delete statistical records associated with an object database that no longer exists.

To start a delete statistics operation, type **delstrecs** on the CWM console command line. You are asked to indicate a retention period in days. Records older than the specified number of days are deleted. More recent records are retained.

To delete all records not associated with an active object, and to delete all unmatched records regardless of age, type a zero when prompted for retention period. You should perform this operation periodically to clean out the statistics database.

Launching Summary Reports

To launch summary reports, complete the following procedure:

Step 1 Open a terminal window.

Step 2 Enter the **NWReport** command at the prompt.

The summary report window (see Figure 9-3) displays statistical and graphical data for the selected report type.

Configuring Summary Reports

This section describes how to use summary reports.

Select a report type option from either the **Resource Capacity** or **Performance Data** menus. When you select the **Resource Capacity** menu's **Network Report** option, a statistical and graphical view of the resources being utilized at every node in the network is displayed in the **Result** pane in this window.

Select any of the **Performance Data** menu's options for a list of report filters available through Connection - Connection Traffic Summary, Connection - Connection Traffic Dropped, Trunk - Trunk Traffic, or Port - Port Traffic Summary windows, respectively. You need to select the desired report filter options in these windows, then click on the **Plot** button. The statistical and graphical data is then displayed in the Report Application window.

Note Unlike the Wingz application, only one report is displayed at a time.

When a report is displayed in the **Result** pane, print or save it in an ASCII file.

File—Save Menu Option

Select this option to save the data used to plot the graph into a CSF (Comma Separated Format) file you specify. When multiple graphs are displayed, each graph is saved in a separate file. A unique file name is created by appending a number to the file name specified. The graphs are numbered left to right. Each file has a ".csf" extension and the files are saved in the /usr/users/svplus/report directory.

File—Print Menu Option

Select this option to choose a printer or file name. Select file name, and a postscript image is saved to the /usr/users/svplus/report/<*file_name*>.ps file, where <*file_name*> is the name of the file specified. When multiple graphs or tables are displayed on the screen, all graphs or tables are saved in the same file.

File—Exit Menu Option

Select this option to terminate the Report Application. The Report Application window is closed.

Resource Capacity—Network Report Menu Option

Select this option to display basic node information for all nodes in the network in the Network Report window. This report provides a view of the resources being utilized at every node in the network.

Resource Capacity—Top Utilization Report Menu Option

Select this option to display the top utilized trunks, ports, or connections for the entire network or a specified node.

Performance Data—Connection - Connection Traffic Summary Menu Option

Select this option to specify the connection to be plotted and the plot duration through the Connection Traffic Summary window.

Upon specifying the desired report options and clicking on the **Plot** button, the total traffic transmitted and received, as well as, the availability for a selected PVC are displayed in the Report Application window. Data for both ends of the connection are plotted side by side in this window.

Performance Data—Connection - Connection Traffic Dropped Summary Menu Option

Select this option to specify the connection to be plotted and the plot duration through the Connection Traffic Dropped window.

Upon specifying the desired report options and clicking on the **Plot** button, the totals of the dropped traffic for a selected PVC are displayed in the Report Application window. Data for both ends of the connection are plotted side by side in this window.

Note The Connection Traffic Dropped Summary menu option is not currently supported for CESM cards.

Performance Data—Trunk -Trunk Traffic Summary Menu Option

Select this option to specify the trunk to be plotted and the plot duration through the Trunk Traffic Summary window.

Upon specifying the desired report options and clicking on the **Plot** button, the total traffic transmitted and received and the unavailability for a selected trunk are displayed in the Report Application window. Data for both ends of the trunk are plotted side by side.

Note For Cisco MGX 8220 feeder trunks, only the routing node end of the trunks are supported as the Cisco MGX 8220 end-point does not support the required statistic types.

Performance Data—Port - Port Traffic Summary Menu Option

Select this option to specify the port to be plotted and the plot duration through the Port Traffic Summary window.

Upon specifying the desired report options and clicking on the **Plot** button, the total traffic transmitted and received and the unavailability for a selected port are displayed in the Report Application window. Data for both ends of the port are plotted side by side.

Note For Cisco MGX 8220 feeder trunks, only the routing node end of the trunks are supported as the Cisco MGX 8220 end-point does not support the required statistic types.

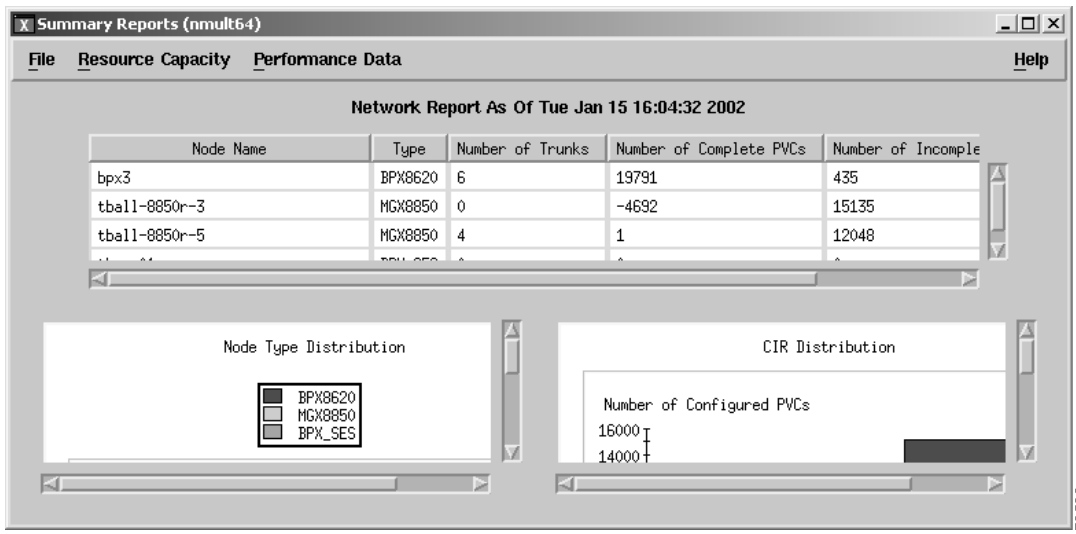
Result Pane

This pane is used to display statistical and graphical data, as well as status and error messages.

Network Report

The Network Report window is displayed when you select the **Resource Capacity** menu's **Network Report** option in the Summary Reports application window, as shown in Figure 9-3. This report provides you a view of the resources being utilized at every node in the network.

Figure 9-3 Network Report Window



This is a two part report. The report's top half displays statistical information in tabular format for each node in the network. The following information is listed for each node:

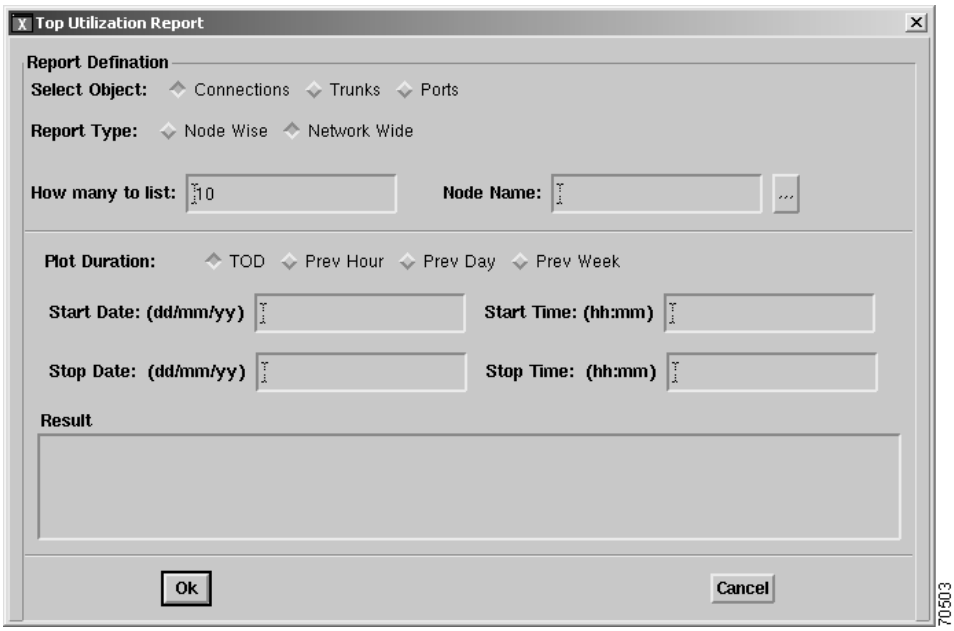
- node name
- node type
- number of trunks on this node
- number of completed connections originating/terminating on this node
- number of incomplete connection on this node (part of a multi-segment connection)
- total CIR originating/terminating on this node

The report's bottom portion displays two graphs. The first graph is a pie chart displaying the break-down by node type (Cisco BPX 8600, Cisco MGX 8220, Cisco MGX 8800, Cisco IGX 8400, or other). The second graph displays the CIR distribution in the network.

Top Utilization Reports

The Top Utilization Reports is displayed when you select the **Resource Capacity** menu's **Top Utilization Report** option in the Report Application window, as shown in Figure 9-4. The Top Utilization Report lists as the top 10 (or as many as you select with a maximum of 50) utilized trunks, ports, or PVCs depending on which object is selected. The user can specify a network wide report or a report for a given node. The user also can specify the number of top utilized objects. In addition, if the user specifies a report for a given node, then the node must be specified.

Figure 9-4 Top Utilization Report Window



After the report is generated, a bar graph is displayed giving the respective utilization of each port, trunk, or PVC.

When you select to list the Top Utilized Trunks, the report application retrieves the required statistics, described in Table 9-2, and performs the following calculations for each trunk:

- percent bytes received from the network (number of packets/cells) received per second/line load) * 100.
- percent bytes transmitted to the network (number of packets/cells) transmitted per second/line load) * 100.
- percent utilization of the trunk = percent bytes received from the network + percent bytes transmitted to the network.

Table 9-2 Required Statistics for Top Utilized Trunks Report

Trunk Type	Percentage of Cells Received (Stats ID)	Percentage of Cells Received (Stats ID)
Narrow Band	—	Total packets transmitted (23)
Cisco IGX 8400-ATM	Total cells received (38)	Total cells transmitted (37)
Cisco BPX 8600-ATM	BXM: Total Cells Rx (219	Total cells transmitted to line (52)

Report Definition Pane

This Report Definition pane is comprised of the following components:

Select Object

Click on the button **Connections**, **Trunks**, or **Ports** to select the object for report generation.

Report Type

Choose either the network wide or node report. The default is **network wide**.

How many to list

Specify the number of objects to be listed in the report. The default is **10** and the maximum is **50**.

Node Name

Specify the node and interface shelf names if the report is for a node only. Click on the "**...**" button to display the Node: Shelf Selection window. Select a node name and corresponding shelf name from this window. This area is inactive if you have selected a network wide report.

Plot Duration

Selections for time of day (**TOD**), previous hour (**Prev Hour**), previous day (**Prev Day**), and previous week (**Prev Week**) are displayed. Indicate the Start Date and Stop Date in dd/mm/yy (day/month/year) format and the Start Time and Stop Time in hh.mm (hour.minute) format.

OK

Choose this button to generate the report.

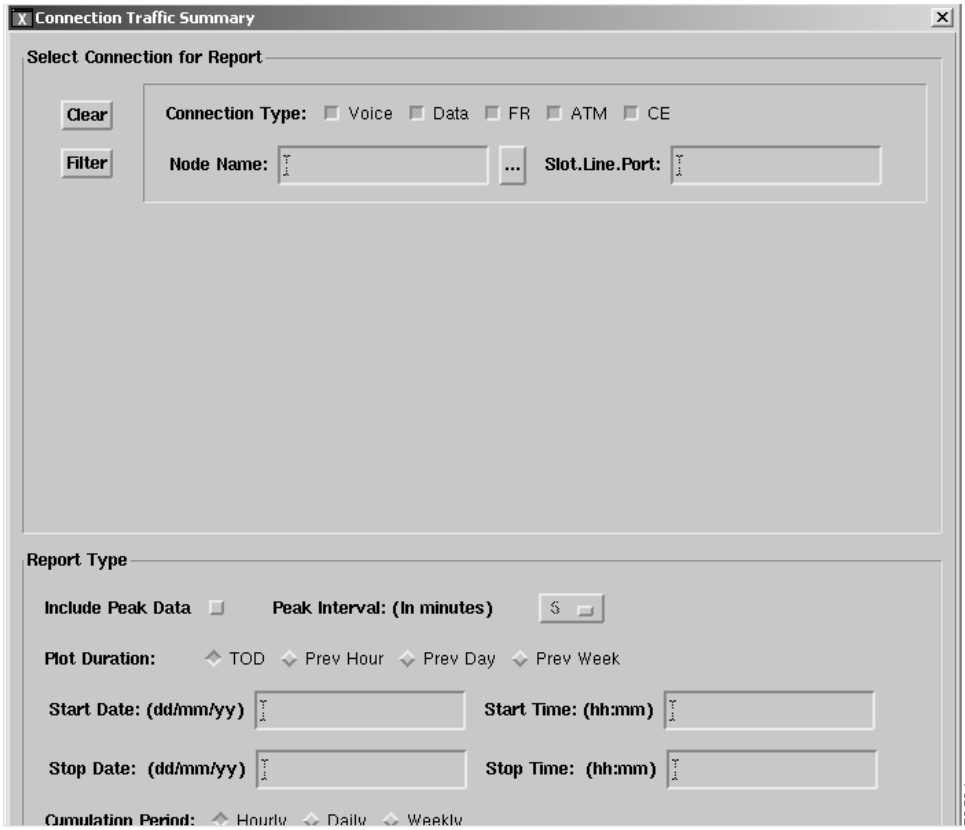
Cancel

Choose this button to clear all fields and return to the Report Main Window.

Connection Traffic Summary

The Connection Traffic Summary window is displayed when you select the **Performance Data** menu's **Connection Traffic Summary** option from the **Connection** submenu in the Performance Data's menu, as shown in Figure 9-5. You must select a PVC and plotting time interval, then click on the **Plot** button to have the statistical information pertaining to connection traffic, plotted into graphs for both ends of the connection and displayed in the Report Application window.

Figure 9-5 Connection Traffic Summary Window



The statistic types used to plot this report are based on the end-point type of the connection. Table 9-3 describes the statistic types needed. The Report Application retrieves all instances (within the plot period) of the statistic types from the database and calculates the following:

- percent received from the network = (number of bits per second / CIR) * 100
- percent transmitted to the network = (number of bits per second / CIR) * 100
- percentage of time in service = (seconds in service / (bucket interval * 60)) * 100

The following conversions are used to convert to bits per second:

- for FR endpoints, convert bytes received to bits per second (number of bytes received / (bucket interval * 60)) * 8
- for ATM/CE endpoints, convert cells received to bits per second, using **Connection Manager's** conversion formula (each cell has a 48 byte payload)
  - bps = (number cells received / (bucket interval * 60)) * 48 * 8
- for VOICE/DATA endpoints, convert packets to bits per second (each packet has 24 bytes)
  - bps = ((number packets received / (bucket interval * 60)) * 24 * 8

When the **Include Peak Data** button is enabled, the percent peak values of the total traffic transmitted and received for a selected PVC are displayed along with the average values in the same graph. The average raw counts are displayed in tabular form.

Data for both ends of the connection are plotted side by side. The statistic types used to plot this report are based on the end-point type of the connection. The Report Application retrieves peak instances (within the plot period) of all statistic types from the database and calculates the following:

- peak number of bytes received from the network (in percentage of CIR) = (peak number of bits received per second / CIR) * 100
- peak number of bytes transmitted to the network (in percentage of CIR) = (peak number of bits transmitted per second / CIR) * 100

The following conversions are used to convert to bits per second:

- For FR endpoints, convert bytes received to bits per second (peak number of bytes received * 8) / (peak interval * 60)
- for ATM/CE endpoints, convert cells received to bits per second, using **Connection Manager**'s conversion formula (each cell has a 48 byte payload)
  - peak bps = (peak number cells received * 48 * 8) / (peak interval * 60)
- for VOICE/DATA endpoints, convert packets to bits per second (each packet has 24 bytes)
  - peak bps = (peak number packets received * 24 * 8) / (peak interval * 60)

Table 9-3 Required Statistics for Connection Traffic Summary Report

End-point Type	Percentage of Bytes Received (Stats ID)	Percentage of Bytes Transmitted (Stats ID)	Percentage of Time in Service (Stats ID)
FR	Bytes received (9)	Bytes transmitted (11)	Seconds In Service (16)
ASI - ATM	Cells received Port (29)	Cells transmitted Port(45)	—
AUSM - ATM	Total cells received (68)	Total cells transmitted (61)	Seconds In Service (16)
Cisco MGX 8220 - CE	Total cells received (72)	Total cells transmitted (71)	—
Voice	Packets received (4)	Packets transmitted (6)	Seconds In Service (16)
Data	Packets received (4)	Packets transmitted (6)	Seconds In Service (16)

Select Connection for Report Pane

This Select Connection for Report pane is comprised of the following components:

Clear Button

Click on this button to clear the **Connection Identifier** pane and return to the default settings.

Filter Button

Click on this button to populate the **Connection Identifier** pane with the connections matching the report filter options specified.

Connection Type Buttons

Click on a button (**Voice, Data**, **FR**, **ATM**, or **CE**) to select that particular connection type. A list of the connections corresponding to that connection type are displayed in the **Connection Identifier** pane once you click on the **Filter** button. By default, all connection types are selected.

Node Name

Specify the node and interface shelf names for the end point in this field. Click on the "**...**" button to display the Node:Shelf Selection window. Select a node name and corresponding shelf name from this window. The default is all connections (this field is blank).

Slot.Line.Port

Specify the end-point's slot and port numbers in this field. The default is all ports (this field is blank).

Connection List

This region is populated when you select the **Filter** button. All connections matching the filter criteria are displayed in this region. Select a single entry from the list for plotting.

Each entry in the list has the following format:

Connection Identifier—the local and remote endpoints are displayed in this column. When certain fields are not applicable, "**..**" is displayed. For example, for routing nodes, <*interfaceshelfname*> is displayed as "**..**".

- The format of the endpoints is as follows:
  - For Frame Relay: <*nodename*>.<*interfaceshelfname*>.<*slot*>.<*line*>.<*port*>.<*DLCI*>
  - For ATM: <*nodename*>.<*interfaceshelfname*>.<*slot*>.<*line*>.<*port*>.<*vpi*>.<*vci*>
  - For CE, Voice, and Data: <*nodename*>.<*interfaceshelfname*>.<*slot*>.<*line*>.<*port*>
- **Type**—the end-point types for the local and remote ends are displayed in this column.
- **CIR**—the CIRs for the local and remote ends are displayed in this column.

Report Type Pane

The Report Type pane is comprised of the following components:

Include Peak Data

Specify Include Peak Data along with Peak Interval to display the highest value in that interval.

Peak Interval

Select peak intervals from the values of 1, 5, 6, 10, 12, and 15 minutes if the Include Peak Data button has been enabled. The default value is 5 minutes (300 seconds).

Note You must select the same peak interval as the one enabled during statistics collection.

Plot Duration

Selections for time of day (**TOD**), previous hour (**Prev Hour**), previous day (**Prev Day**), and previous week (**Prev Week**) are displayed. The default value is **TOD**.

When you select **Prev Hour**, **Prev Day**, or **Prev Week**, the **Start Date/Start Time** fields are inactive, and when the **Stop Date/Stop Time** fields are blank, they are populated with the current date and time. When you modify the stop date/time, the modified value is used for the plot duration. When you select **TOD**, both **Start Date/Start Time** and **Stop Date/End Time** fields are activated, and the **Stop Date/End Time** fields are populated with the current date and time.

Start Date/Start Time

Specify the starting date and time for the graph in this field.

Stop Date/End Time

Specify the stop date and time for the graph in this field.

Cumulation Period

Click on the appropriate button (**Hourly**, **Daily**, or **Weekly**) to set the report's plot interval. The default selection is **Hourly**.

Result Pane

The Result Pane displays status and error messages:

Plot Button

Click on this button to initiate the plotting of the report. The data and graphs are displayed in the Report Application window.When statistic entries are not found, an error message is displayed in the **Result** pane. Otherwise, the **Result** pane displays the number of entries found.

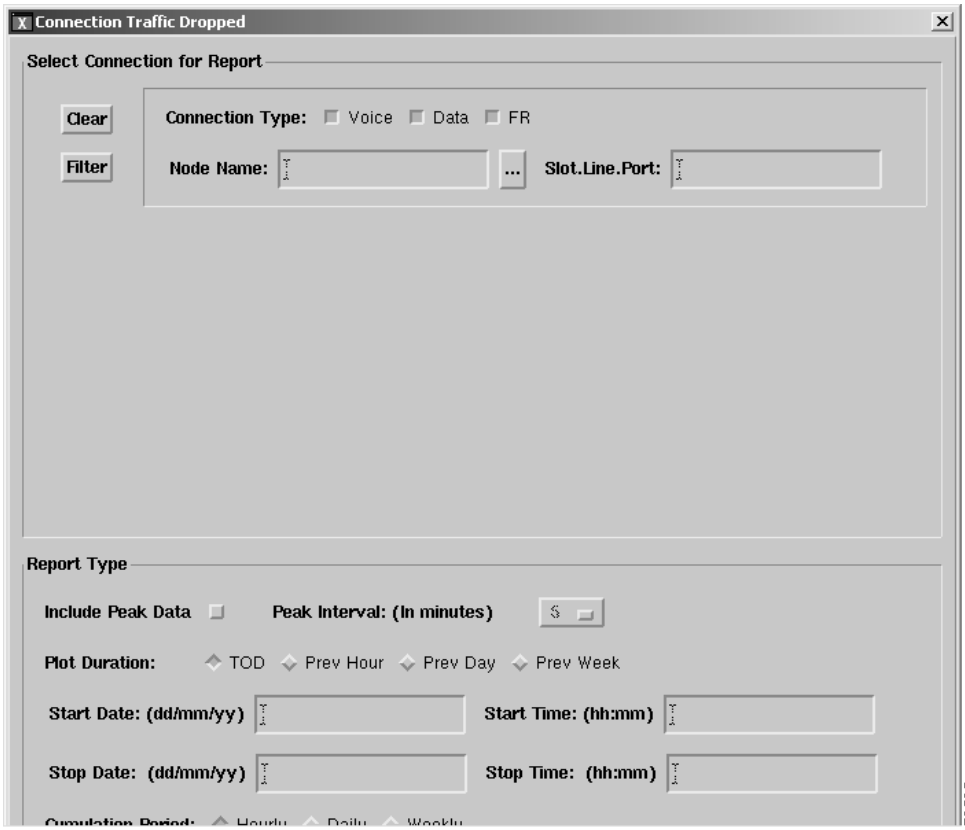
Cancel Button

Click on this button to cancel the current report filter operation and close this window.

Connection Traffic Dropped Window

The Connection Traffic Dropped window is displayed when you select the **Performance Data** menu's **Connection Traffic Dropped** option from the **Connection** submenu in the Performance Data's menu, as shown in Figure 9-6. You must select a PVC and plotting time interval, then click on the **Plot** button to have the statistical information pertaining to the total traffic dropped for a selected PVC, plotted into graphs for both ends of the connection and displayed in the Report Application window.

Figure 9-6 Connection Traffic Dropped Window



The statistic types used to plot this report are based on the end-point type of the connection. Table 9-4 describes the statistics types needed. The Report Application retrieves all instances (within the plot period) of the statistics types from the database and calculates the following:

- Percentage of received bytes dropped = (number of bps of received bytes dropped / CIR) * 100
- Percentage of transmitted bytes dropped = (number of bps of transmitted bytes dropped / CIR) * 100

When the **Include Peak Data** button is enabled, the percent peak values of the dropped traffic for a selected PVC are displayed. Data for both ends of the connection are plotted side by side. The statistic types used to plot this report are based on the end-point type of the connection. The Report Application retrieves statistics from the database and calculates the following:

- Peak number of bytes received bytes dropped (in percentage of CIR) = (peak number of bits received per second) / CIR) * 100
- Peak number of bytes transmitted dropped (in percentage of CIR) = (peak number of bits transmitted per second) / CIR) * 100

The following conversions are used to convert to bits per second:

- For FR endpoints, convert bytes received to bits per second (peak number of bytes received * 8) / (peak interval * 60)
- For ATM/CE endpoints, convert cells received to bits per second, using **cmgrd**'s conversion formula (each cell has a 48 byte payload)

  peak bps = (peak number cells received * 48 * 8) / (peak interval * 60)

- For VOICE/DATA endpoints, convert packets to bits per second (each packet has 24 bytes)

  peak bps = (peak number packets received * 24 * 8) / (peak interval * 60)

Note Cells discarded is not supported on ASI and AUSM.

Table 9-4 Required Statistics for Connection Traffic Dropped Report

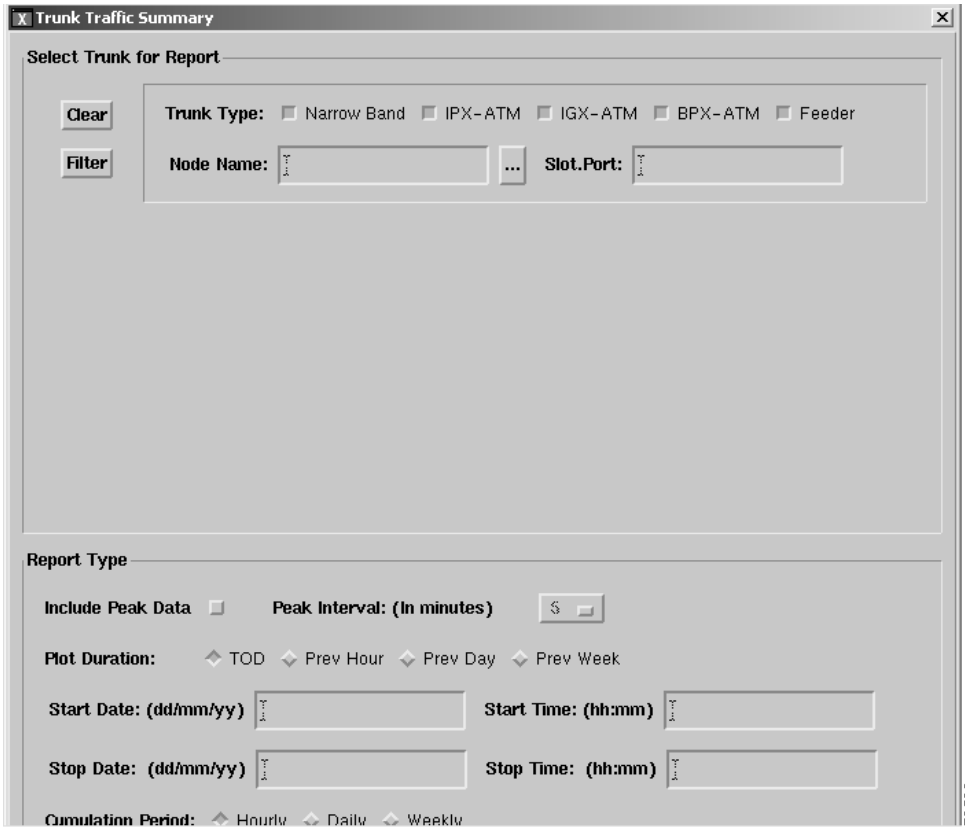
End-point Type	Percentage of Received Bytes Discarded (Stats ID)	Percentage of Transmitted Bytes Discarded (Stats ID)
FR	Received bytes discarded (10)	Transmitted bytes discarded (12)
ASI - ATM	—	—
AUSM - ATM	—	—
Voice	Received bytes discarded (5)	—
Data	Received bytes discarded (5)	—

Trunk Traffic Summary Window

The Trunk Traffic Summary window is displayed when you select the Performance Data menu's Trunk Traffic Summary option in the Report Application window, as shown in Figure 9-7. You must select a trunk type and plotting time interval, then click on the Plot button to have the statistical information pertaining to the trunk traffic, plotted into graphs and displayed in the Report Application window.

Note For Cisco MGX 8220 feeder trunks, only the routing node end of the trunks are supported as the Cisco MGX 8220 end-point does not support the required statistic types.

Figure 9-7 Trunk Traffic Summary Window



The statistic types used to plot this report are based on the trunk's end-point type. Table 9-5 describes the statistic types needed. The Report Application retrieves all instances (within the plot period) of the statistics types from the database and calculates the following:

- percentage of bytes received from network = (number of packets or cells received per second / line load) * 100
- percentage of bytes transmitted to the network = (number of packets or cells transmitted per second / line load) * 100
- percentage of time unavailable = (unavailable seconds / (bucket interval * 60)) * 100

When the **Include Peak Data** button is enabled, the percent peak values of the total traffic transmitted and received for a selected trunk are displayed. The percent peak values are plotted in the same graph with the percent average data. Data for both ends of the trunk are plotted side by side. The Report Application retrieves statistics from the database and calculates the following:

- peak number of bytes received from the network (in percentage of line load) = ((peak number of packets or cells received) / (peak interval * line load)) * 100
- peak number of bytes transmitted to the network (in percentage of line load) = ((peak number of packets or cells transmitted) / (peak interval * line load)) * 100

The statistic types used to plot this report are based on the end-point type of the connection.

Table 9-5 Required Statistics for Trunk Traffic Summary Report

Trunk Type	Percentage of Cells Received (Stats ID)	Percentage of Cells Transmitted (Stats ID)	Percentage Unavailable (Stats ID)
Narrow band	—	Total packets transmitted (23)	—
Cisco IPX - ATM	Total cells received from line (68)	Total cells transmitted to line (61)	Unavailable Seconds (39)
Cisco IGX 8400 - ATM	Total cells received (38)	Total cells transmitted (37)	—
Cisco BPX 8600 - ATM	BXM: Total Cells Rx (219)	Total cells transmitted to line (52)	Unavailable Seconds (39)

Select Trunk for Report Pane

The Select Trunk for Report pane is comprised of the following components:

Clear Button

Click on this button to clear the **Trunk Identifier** pane and return to the default settings.

Filter Button

Click on this button to populate the **Trunk Identifier** pane with the trunks matching the report filter options specified.

Trunk Type

A set of toggle buttons corresponding to the trunk types supported (**Narrow Band**, **IPX-ATM**, **IGX 8400-ATM**, **BPX 8600-ATM**, and **Feeder**) are displayed in this area. By default, all trunk types are selected.

Node Name

Specify the node and interface shelf names for the local end point in this field. Click on the "**...**" button to display the Node: Shelf Selection window. Select the node name and corresponding shelf name from this window. The default is all nodes (the field is blank).

Slot.Port

Specify the end-point's slot number in this field. The default is all slots (the field is blank).

Trunk List

This region is populated when you select the **Filter** button. All trunks matching the filter criteria are displayed in this region. A single entry from the list for plotting can be selected.

Each entry in the list has the following format:

- **Trunk Identifier**—the local and remote endpoints are displayed in this column. The format of the endpoints is as follows: <*nodename*>.<*slot*>.<*port*>.<*vtrk*>
- **Card Type**—the end-point card type for the local and remote ends are displayed in this column.
- **Load**—the line loads for the local and remote ends are displayed in this column.

Report Type Pane

The Report Type pane is comprised of the following components:

Include Peak Data

Specify Include Peak Data along with Peak Interval to display the highest value in that interval.

Peak Interval

Select peak intervals from the values of 1, 5, 6, 10, 12, and 15 minutes if the Include Peak Data button has been enabled. The default value is 5 minutes (300 seconds).

Note You must select the same peak interval as the one enabled during statistics collection.

Plot Duration

Selections for time of day (**TOD**), previous hour (**Prev Hour**), previous day (**Prev Day**), and previous week (**Prev Week**) are displayed. The default value is **TOD**.

When you select **Prev Hour**, **Prev Day**, or **Prev Week**, the **Start Date/Start Time** fields are inactive, and when the **Stop Date/Stop Time** fields are blank, they are populated with the current date and time. When you modify the stop date/time, the modified value is used for the plot duration. When you select **TOD**, both **Start Date/Start Time** and **Stop Date/End Time** fields are activated, and the **Stop Date/End Time** fields are populated with the current date and time.

Start Date/Start Time

Specify the starting date and time for the graph in this field.

Stop Date/End Time

Specify the stop date and time for the graph in this field.

Cumulation Period

Click on the appropriate button (**Hourly**, **Daily**, or **Weekly**) to set the report's plot interval. The default selection is **Hourly**.

Result Pane

Status and error messages are displayed in this pane.

Plot Button

Click on this button to initiate the plotting of the report. When statistic entries are not found, an error message is displayed in the **Result** pane. Otherwise, the **Result** pane displays the number of entries found.

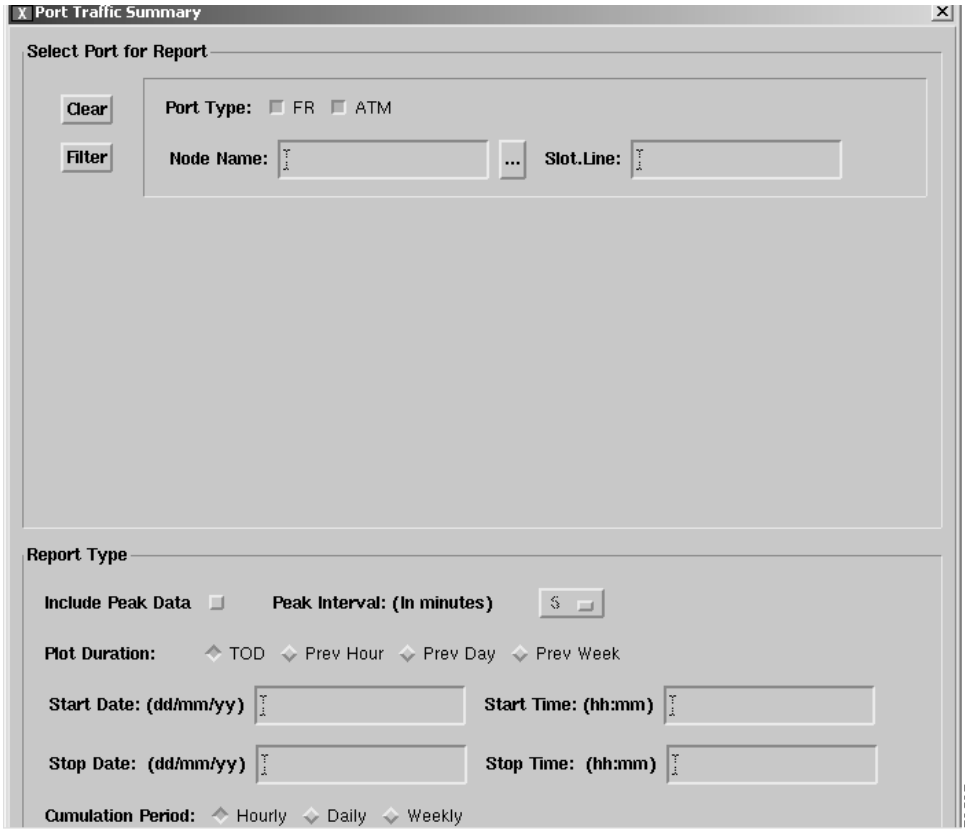
Cancel Button

Click on this button to cancel the current report filter operation and close this window.

Port Traffic Summary Window

The Port Traffic Summary window is displayed when you select the **Performance Data** menu's **Port Traffic Summary** option in the Report Application window, as shown in Figure 9-8. You must select a port type and plotting time interval, then click on the **Plot** button to have the statistical information pertaining to the port traffic, plotted into graphs and displayed in the Report Application window.

Figure 9-8 Port Traffic Summary Window



Required statistics for port traffic are described in Table 9-6. The report application retrieves all instances of the statistics types within the selected plot period from the database and calculates the following:

- Percentage of bytes received from the network = (number of bits received per second / port speed) * 100
- Percentage of bytes transmitted to the network = (number of bits transmitted per second / port speed) * 100

The following conversions are used to convert to bits per second:

- Frame Relay ports bytes received to bits per second = (number of bytes received / (bucket interval * 60)) * 8
- ATM ports convert cells to bits per second: bps = (number of cells received / (bucket interval * 60)) * 48 * 8
- Voice ports: bps = ((number of packets received / (bucket interval * 60)) * 24 *8

When the **Include Peak Data** button is enabled, the percent peak values of the total traffic transmitted and received for a selected port are displayed along with the average values in the same graph. The average raw counts are displayed in tabular form. The statistic types used to plot this report are based on the port type. The Report Application retrieves peak instances (within the plot period) of all statistic types from the database and calculates the following:

- Peak number of bytes received from the network (in percentage of port speed) = (peak number of bits received per second / port speed) * 100
- Peak number of bytes transmitted to the network (in percentage of port speed) = (peak number of bits transmitted per second / port speed) * 100

Table 9-6 Required Statistics for Port Traffic Summary

Port Type	Percentage Bytes Received (Stats ID)	Percentage Bytes Transmitted (Stats ID)
Cisco IGX 8400 Frame Relay (FRP, FRM, and UFM)	Number of Bytes Received (2)	Number of Bytes Transmitted (3)
Cisco BPX 8600 ATM (ASI, BXM)	Number of Cells Received (7)	Number of Cells Transmitted (11)
Cisco MGX 8220 Frame Relay (FRSM)	Number of Bytes Received (2)	Number of Bytes Transmitted (3)
Cisco MGX 8220 ATM (AUSM)	Total Number of Cells Received from Line (40)	Total Number of Cells Transmitted from Line (41)
Voice (UVM, CVM, CDP)	Number of Voice Packets Received (61)	Number of Voice Packets Transmitted (60)

Select Port for Report Pane

The Select Port for Report pane is comprised of the following components:

Clear Button

Click on this button to clear the **Port Identifier** pane and return to the default settings.

Filter Button

Click on this button to populate the **Port Identifier** pane with the ports matching the report filter options you specified.

Port Type

A set of toggle buttons corresponding to the port types supported (**Frame Relay**, **ATM,** and **Voice**) are displayed in this area. By default, all port types are selected.

Node Name

Specify the node name for the local end point in this field. Click on the "**...**" button to display the Node:Shelf Selection window. Select the node name and corresponding shelf name from this window. The default is all nodes (the field is blank).

Slot.Line

Specify the endpoint's slot and line number in this field. The default is all slots (the field is blank).

Port List

This region is populated when you select the **Filter** button. All ports matching the filter criteria are displayed in this region. You may select a single entry from the list for plotting.

Each entry in the list has the following format:

- **Port Identifier**—the local and remote endpoints are displayed in this column. The format of the endpoints is as follows: <*nodename*>.<*slot*>.<*line*>.<*port*>
- **Port Type**—the type of the selected port is displayed in this column.
- **Port Speed**—the port speed for the selected port is displayed in this column.

Report Type Pane

The Report Type pane is comprised of the following components:

Include Peak Data

When enabled peak performance is included in the graph along with the average performance data.

Peak Interval Option

Use this to select peak intervals from the values of 1, 5, 6, 10, 12, and 15 minutes if you have enabled the Include Peak Data button. The default value is 5 minutes (300 seconds).

Note You must select the same peak interval as the one enabled during statistics collection.

Plot Duration

Selections for time of day (**TOD**), previous hour (**Prev Hour**), previous day (**Prev Day**), and previous week (**Prev Week**) are displayed. The default value is **TOD**.

When you select **Prev Hour**, **Prev Day**, or **Prev Week**, the **Start Date/Start Time** fields are inactive, and when the **Stop Date/Stop Time** fields are blank, they are populated with the current date and time. When you modify the stop date/time, the modified value is used for the plot duration. When you select **TOD**, both **Start Date/Start Time** and **Stop Date/End Time** fields are activated, and the **Stop Date/End Time** fields are populated with the current date and time.

Start Date/Start Time

Specify the start date and time for the graph in this field.

Stop Date/End Time

Specify the stop date and time for the graph in this field.

Cumulation Period

Click on the appropriate button (**Hourly**, **Daily**, or **Weekly**) to set the report's plot interval. The default selection is **Hourly**.

Result Pane

Status and error messages are displayed in this pane.

Plot Button

Click on this button to initiate the plotting of the report. When statistic entries are not found, an error message is displayed in the **Result** pane. Otherwise, the **Result** pane displays the number of entries found.

Cancel Button

Click on this button to cancel the current report filter operation and close this window.

CHAPTER 10

Network Configurator

This chapter describes the CWM Network Configurator desktop application. The Network Configurator is a new Java-based application for Release 10 of CWM that enables users to add new nodes, or modify or delete existing nodes. It is also used to provide descriptor information, node name, and IP address information for the nodes in your network.

Note Every time a new session of the Network Configurator is started, you must edit the **Topod.conf** file located in the **/usr/users/svplus/config** directory in order to disable automatic unique node ID generation. The third line of **Topod.conf** describes the next line as the Auto Node Id Generation flag. On line four, change the **TRUE** to **FALSE** to disable automatic node ID generation.

How to Start the Configurator

The Network Configurator is started by entering runConfigurator <*machine name*> **<*login*>** <*password*> on a shell's command line, where Cisco WAN Manager Release 10 is installed**.**

The Network Configurator main window appears, allowing the user to add, delete, and modify nodes.

Adding Nodes

To add a new node, complete the following steps:

Step 1 To add a node, select **Edit** from the main menu bar of the Network Configurator window.

Step 2 Select **Node** from the **Edit** menu.

Step 3 Select **Add** from the **Node** menu.

Step 4 A **Node Dialog** box appears after selecting **Add** from the **Node** menu. The Node Dialog box contains two tab windows, **Node** and **Other Info**, in which the user enters information about the new node.

Step 5 In the **Node** window enter the new node name, the node Descriptor information, and FTP information, in the appropriate fields.

Step 6 In the **Other Info** window enter the mode, (Connected or Stand Alone), the MGX Model, the IP Address, and any Parent Information, including Feeder Slot, Feeder Port, Parent Name, Parent Slot, and Port.

Step 7 Press the **OK** button in the Node Dialog box.

The Network Configurator validates the new node by ensuring its IP address and unique node name. The node will be displayed in the Network Configurator main window if the node information is valid.

Step 8 Select **close** from the Node Dialog pull down menu, located in the upper left hand corner of the window.

Step 9 Select **File**, then **Save** from the Network Configurator Window.

Note Changes made using the Network Configurator are not saved in the **node_info** table until you select **Save** from the file menu. If the **Cancel** button is pressed, no changes will be made to the **node_info** table.

Deleting Nodes

To delete a node, complete the following steps:

Step 1 Select the node to be deleted from the expanded node tree of the Network Configurator window.

Step 2 Select **Edit** from the main menu bar of the Network Configurator window.

Step 3 Select **Node** from the **Edit** menu.

Step 4 Select **Delete** from the **Node** menu.

Step 5 Select **File**, then **Save** from the Network Configurator window.

If the node has been successfully deleted, it will disappear from the Network Configurator main window.

Note Only Stand Alone nodes can be deleted.

Modifying Nodes

To modify a node, complete the following steps:

Step 1 Select the node to be modified from the expanded node tree of the Network Configurator window.

Step 2 Select **Edit** from the main menu bar of the Network Configurator window

Step 3 Select **Node** from the **Edit** menu.

Step 4 Select **Modify** from the **Node** menu.

Step 5 A **Node Dialog** box appears after selecting **Modify** from the **Node** menu. The Node Dialog box contains two tab windows, **Node** and , in which the user can modify information about the node.

Step 6 In the **Node** window, modifiable fields include SNMP community strings, FTP information, and Custom information.

Step 7 In the **Mode** window there are no modifiable fields.

Step 8 Press the **OK** button in the Node Dialog box.

Step 9 Select **close** from the Node Dialog pull down menu, located in the upper left hand corner of the window.

Step 10 Select **File**, then **Save** from the Network Configurator window.

Note Changes made using the Network Configurator are not saved in the **node_info** table of the database until you press the **Save** button. If the **Exit** button is pressed, no changes will be made to the **node_info** table. The new node information is updated on the expanded node tree of the Network Configurator window. Contents of the **node_info** table should only be displayed or edited through the Network Configurator.

Note Only one instance of the Network Configurator should be used at a time for performing an operation. CWM provides tools that generate a unique node ID, but if multiple sessions of the Configurator are used at the same time, problems will occur.

Community String Configuration

Release 10.4 of CWM allows the configuration of community strings for SNMP management. CWM supports various multi-service-switching devices. Prior to the 10.4 release, CWM supported configurable SNMP community string settings for MGX8850/R2 nodes only. The CWM application **Network Configurator** is used to configure SNMP community strings from MGX8850/R2 devices. All other devices use default SNMP community strings from the **svplus.config** file. For some devices such as MGX8220 and MGX8850/R1 SNMP, the community strings are hard coded from the device side.

The community strings on the devices and the community strings used by CWM do not sync up automatically (except at the initial stage when the community strings on the devices are at default). Users have to explicitly change them on both sides (using the **Network Configurator** on CWM). If this is not done, all SNMP requests (including RTM) will fail, and CWM's database be inconsistent with the network.

Note The Runconfig does not require the CWM core to be running; it can be used when it is up and running or when it's down.

To Configure Community Strings:

Step 1 Change the community strings on the devices via CLI. You will need to telnet to the switch to configure the community strings at the switches.

Step 2 Use the CWM **Network Configurator** to change the community strings, then choose **Save** from the menu. After saving, the CWM processes use the new community strings for SNMP accesses. The Primary CWM also sends the configured community strings to other Secondary CWMs through the CWM Gateways.

Since users have to configure the community strings on both the devices (via CLI), and at the CWM stations (via Configurator), there is a possibility of typing in mismatched community strings. This would result in the node with the mismatched community strings appearing to be un-reachable to CWM.

Note Add, modify and delete can only be done from the Primary CWM.

Note Configured community strings cannot contain underscore (_) or “at” signs (@). Also, spaces are not allowed in community strings and ftp passwords.

Note You must enter community strings on a **Network Configurator** that pertains to the database of a primary CWM station.

CHAPTER 11

CWM to CWM Communications

Release 10 of Cisco WAN Manager has been designed to enable multiple CWM workstations to manage a network with improved network synchronization and scalability. Due to the size and growth of networks, it is faster to retrieve initial user data from another CWM workstation that is already running and synchronized with the network. An industry standard CORBA architecture is used in Release 10 of CWM to implement the communications between two or more CWM workstations. The architecture uses a server-client structure for communications between the CWM server and client processes.

CWM workstations use CWM-CWM Communications to synchronize user data with each other. When user data is provisioned or changed, the CWM workstations will propagate the new data to the other CWM workstations. The user is able to continue the provisioning of network data, even when communications between a Primary CWM and Secondary CWM have been interrupted. If for any reason the communications between CWM servers are interrupted, the provisioning of the user data will be suspended on the Secondary CWM, but not on the Primary CWM as user data provisioning will continue on the Primary CWM. During that time, the provisioning of user data and monitoring of the network are not impacted. This is called the Degraded Mode of Operation. This chapter introduces the CWM-CWM Communications feature and also procedures for recovering from failures that may cause the CWM to run in Degrade Mode.

Note CWM to CWM Communications does not affect network sync-up.

CWM Domain

A CWM domain consists of all CWM workstations in a network that are in communication with each other. Each CWM workstation functions as a *CWM gateway*, however one CWM workstation is designated as the *Primary CWM* for keeping the user data, and is the source of all user data that the Secondary CWMs can sync with.

You can define a CWM domain by specifying a list of CWM workstations that will communicate with each other, as described in this chapter under “Configuring CWM to CWM Communications”. All CWM workstations in a given domain must be connected to the same set of networks to ensure that their databases remain consistent.

Note The **network.conf** file does not have to be the same on all CWM stations in the domain as long as the gateway nodes specified in this file are part of the same network. Even though CWMs that manage the same network can talk to each other, managing the same network does not require having identical **network.conf** files on all Secondary and Primary CWMs.

CWMGateway Process

The CWMGateway process provides a communications gateway for CMW workstations. Processes owned by one CWM workstation can communicate with processes owned by another CWM workstation using the CWMGateway process.

CWM workstations within the same CWM domain communicate with other CWM workstations by transferring information between the CWMGateway processes of each CWM workstation. The communication between CWM workstations is set up transparently by the CWMGateway processes in each CWM workstation.

CWM core processes communicate with the CWMGateway process of the CWM workstation to request information from and to send information to another CWM workstation.

CWMGateway Functionality

With the use of the CWMGateway Process, CWM to CWM communications allows CWM to have the following functionality:

- CWM can determine, without the help of the managed network, the presence of other managing CWM servers. This is achieved by having IP connectivity between all CWM workstations.

Note Loss of IP connectivity means that the Primary and Secondary CWMs are not able to communicate through sending or receiving network information, and are not able to ping each other.

- CWM workstations can communicate with other (remote) CWM workstations.
- If a Primary CWM workstation were to be shut down, another CWM workstation would become the new Primary CWM.
- If failure occurs, such as a loss of communication, it can be detected and recovered predictably and reliably.

Apart from the redundancy aspect, one additional benefit of the CWM gateway is the ability for multiple CWM workstations to share User Data, as well as maintain synchronization with the network. The CWM Gateway process maintains consistency of user data across the CWM domain, while the proprietary Robust Trap mechanism and SNMP maintain the CWM database consistent with the network data.

Network Data is defined as data that originates in the network and is communicated to the CWM workstation(s) by means of the proprietary Robust Trap mechanism or by SNMP, depending on the network element concerned. An example of network data is a change in alarm status for a user port or access line.

User Data is information that is supplied by a CWM user, or by an external OSS, and which cannot be stored in a network element and was therefore not visible to other CWM workstations prior to Release 10. Examples of User Data include connection templates, Service Class Templates, SNMP community strings, and the unique node IDs generated by CWM during the network discovery process.

With the CWM gateway function, User Data is propagated between the CWM workstations in a domain, thereby maintaining consistency. The Primary CWM acts as an arbitrator to prevent contention between CWM workstations for the same element of User Data. This means, for example, that if a user on one CWM workstation wants to modify a particular connection template, the Connection Template Manager process on that CWM workstation must request the Primary CWM workstation to lock that resource to prevent concurrent modification by two users.

Establishing Primary CWM and Secondary CWM Priority

In a given wide area network managed by Release 10 of CWM, the first CWM workstation to begin operation will assume the role of Primary CWM. As other CWM workstations become active, they will take on Secondary CWM workstation roles. The only difference in function between Primary and Secondary CWM workstations is that the Primary CWM workstation would provide the Secondary CWM workstations with user data when the Secondary CWM workstation launches.

Priority numbers of all Secondaries are assigned by the Primary at the time a Secondary registers with the Primary. It is based on “first-come-first-serve” logic. All the Secondaries have the same privilege except that the Secondary with priority 1 will take over as the Primary if the Primary shuts down.

The priority numbers of Secondaries might change in a Secondary CWMGateway process’s lifecycle.

In the following cases, the priority numbers among Secondary CWMGateways might change randomly:

- Restart the Primary CWMGateway (by watchdog)
- SwitchOver due to the Primary shutdown
- Primary ForceSwitchOver to a Secondary

This is the result of re-registration with the new Primary CWMGateway process. Priority numbers will be re-assigned by the new Primary CWMGateway process when a Secondary registers with the new Primary. In other words, for whatever reason the Primary CWMGateway process changes, the priority numbers of the Secondaries will be subject to re-assignment.

It is possible that an S2 (Secondary with Priority 2) can become an S1 after the Primary CWMGateway is restarted (by watchdog). It is also possible that an S3 can become an S1 after the switchover.

In the following cases, the priority numbers among Secondary CWMGateways will NOT change randomly:

- Restart a Secondary (by watchdog)
- Shutdown Secondary

In these cases, if Sn (Secondary with priority n) is restarted or shutdown, any Sm (m>n) will become S(m-1), while any Sm (m<n) will remain as Sm.

The difference between these scenarios is that in a Shutdown Secondary case, the Primary CWMGateway process did not change.

Re-establishing Priority after CWM-CWM Communications have been Interrupted

Primary CWM Graceful Shutdown

The first CWM to be launched assumes the role of the primary by default. Subsequently, other CWMs launched will register with the primary CWM and each Secondary CWM is assigned a priority number which identifies the order in which the Secondary CWM was launched with respect to the primary CWM. Before being shutdown gracefully by the user, the CWMGateway on the primary CWM will invoke the IDL interface (used to communicate between two CWMGateway processes), of each of the objects corresponding to a Secondary CWMGateway. This will notify the Secondary CWM that the primary CWM is about to go away and that it will in turn nominate the second CWM in line (priority 1)

to take over as the new primary. The Secondary CWMGateway with priority number 1 (SP1) will now take over as the new Primary, and any remaining CWMGateways will subsequently register with the new Primary CWM. The new CWMGateway priority numbers will be based on "first-come-first-serve" logic.

Note If the Primary CWM is not shut down gracefully, then the Secondary CWM could go into degrade mode. In this case, the user will need to restart the Primary CWM to re-establish the connection between the Primary and Secondary CWMs. The Secondary CWM will then re-sync the user data tables with the restarted Primary CWM as soon as the connection has been re-established.

Note Re-sync between the Secondary CWM and Primary CWM does not depend on how fast the Primary CWM can re-sync with the network after restart. If the Primary CWM has previously discovered all of the nodes in the network, and populated its node_info table with all network node data, it is not necessary for the Secondary CWMs to wait for the Primary CWM to re-sync with the entire network. This capability gives Secondary CWMs in a network the ability to access user data much faster than if they had to wait for the Primary CWM to re-sync with the entire network.

Secondary CWM Graceful Shutdown

A Secondary CWMGateway will notify its primary counterpart before it's shutdown gracefully. The primary CWMGateway will assign a new priority number to the remaining Secondary CWMGateway whose priority number is greater than the priority number of the CWMGateway that has just gone away. The new priority number is one less than the previously assigned priority number. For example, if the CWMGateway with priority number 1 has gone away, the CWMGateway with priority number 2 will be changed to 1 so that it becomes next in line to take over the role of the primary CWM when the current primary CWM goes away.

Configuring CWM-CWM Communications

When a CWM workstation launches, it reads a configuration file called CWMGateway.conf to determine its initial setup and default configurations. Following is an example of a CWMGateway.conf file with a DomainGatewayList of a domain consisting of four CWM workstations named cwmws1, cwmws2, cwmws3, and cwmws4:

```
Debug level 2
DomainGatewayList cwmws1 cwmws2 cwmws3 cwmws4
ForcedSwitchOver cwmws2
HeartBeatInterval 20
```

Parameters in this CWMGateway.conf file must be specified to enable inter-CWM communication; it is the only list of other CWM gateways available to this local host. Each host or CWM workstation listed in the DomainGatewayList must be *reachable* from the local host. Confirm this by using the Unix "ping" command. The host names listed in the DomainGatewayList can be presented in any order.

The CWMGateway.conf file in /usr/users/svplus/config/ specifies the following parameters:

- **Debug level**—tells the CWM gateway how much debugging information to generate. The valid range for this value is 1-5. In a production environment, do not raise this value above 2. The Debug Level is primarily used in engineering development or in a troubleshooting environment with the assistance of technical support.

- **DomainGatewayList**—a list of remote gateways or the other CWM workstations that are part of this CWM domain. These workstations are either running Release 10 of CWM or will be at some point in the future. There must be IP connectivity between all of the CWM workstations listed. The DomainGatewayList parameter lists the CWM workstation hostnames that are part of a given domain and enables communication between these workstations. It is required that all CWM workstations in a domain have the same DomainGatewayList in their CWMGateway.conf file. If a given CWM workstation is the only one managing a network, you do not have to specify this parameter.

Note The **network.conf** file does not have to be the same on all CWM stations in the domain as long as the gateway nodes specified in this file are part of the same network. Even though CWMs that manage the same network can talk to each other, managing the same network does not require having identical **network.conf** files on all Secondary and Primary CWMs.

- **Forced Switchover**—tells a CWM workstation (if it is Primary) to hand over that role to another CWM workstation and become a Secondary CWM workstation. The ForcedSwitchOver parameter indicates a Secondary CWM gateway that assumes the role of Primary CWM gateway when the Primary releases that role. This parameter is only used by the Primary CWM gateway. The Forced Switchover hostname field is empty by default.

Three conditions are required for a forced switchover to take effect:

- The local CWM gateway must be running as the Primary
- The remote CWM gateway designated by the ForcedSwitchOver parameter must be up and running
- The remote CWM gateway designated by the ForcedSwitchOver parameter must have IP connectivity between the Primary CWM gateway and the Secondary CWM gateway

This option is not read at startup or in response to an HUP or USR1 signal, but processed only in response to a USR2 signal.

To initiate a forced switchover follow these steps:

a. Verify that the nominated Secondary host is in the same domain as the Primary host and that CWM is up and running

b. Edit the CWMGateway.conf file manually (with vi or another editor) using the **`ForcedSwitchOver cwmwsx`** command, and set the host name of the nominated Secondary to the ForcedSwitchOver on the Primary

c. Retrieve the process id (pid) of the CWMGateway on the Primary and send a USR2 signal to the CWM gateway on the Primary

- **Heartbeat Interval**—tells the CWM gateway how often to send the heartbeat signal. Values for the Heartbeat Interval must be the same among all CWM workstations in the same domain.The Heartbeat Interval indicates the interval at which the Primary CWM will send the heartbeat signal to the Secondary CWM. If a Secondary CWM fails to detect two consecutive heartbeat signals, it assumes a loss of connectivity with the Primary CWM. There will be no switchover in this situation. The Secondary CWM will log an L1 message, and print an error message on the console, indicating that it has lost connectivity to the Primary CWM. This will be repeated every 60 seconds. It will go back to the normal mode of operation once the heartbeat message has been received. The Secondary CWM will work in a degraded mode of operation until, and unless, the heartbeat is restored with the Primary CWM.

Degrade Mode

The user is able to continue the provisioning of network data, even when communications between a Primary CWM and Secondary CWM have been interrupted. If for any reason the communications between CWM servers are interrupted, user data provisioning will be suspended on the Secondary CWM, but user data provisioning will continue on the Primary CWM. During that time, the provisioning of user data and monitoring of the network are not impacted. This is called the Degraded Mode of Operation.

In order to provide CWM to CWM communications, a CWM workstation must be able to determine, transparently to the network, if another CWM workstation is currently running in the network. This requires IP connectivity between all CWM workstations. If all Secondary CWMs have lost IP connectivity with the Primary CWM, then all Secondary CWMs will function in the degraded mode of operation.

Degrade mode is defined by a loss of connectivity between the Primary CWM and any Secondary CWMs, in which all Secondary CWMs are unable to provision user data, including the adding, deleting, or modifying of user data, while waiting for a connection with the Primary CWM to be restored. In the degrade mode a Secondary CWM can still manage the network data (not user data), and provisioning of network data can still proceed.

Interruption in communications between CWMs may be due to some of the following failures:

- Failure Detection
- Unexpected Exit of the Primary CWMGateway
- Unexpected Exit of the Secondary CWMGateway
- Primary CWM has lost IP or physical connectivity to all Secondary CWMs
- One Secondary CWM has lost IP connectivity with the Primary CWM
- The CWMGateway process dies on the Primary CWM and is not re-started by *watchdog*.
- The CWM workstation crashed or was powered off
- Primary CWM has lost IP or physical connectivity with the only Secondary CWM in a domain
- Loss of Heartbeat from Primary CWMGateway

Recovering From Degrade Mode

Failure Detection

The failure recovery scenario involves handling the unexpected death of either the Primary CWMGateway or a Secondary CWMGateway as well as handling the loss of IP connectivity between the Primary and Secondary CWMGateways. Note, that the CWMGateway process will be launched by *watchdog,* so that it can be automatically restarted if it dies unexpectedly. Also, an Orbix-specific callback mechanism (CORBA::IT_IOCallback) would be used to indicate any break in connection between the Primary CWMGateway and the Secondary CWMGateway processes. This will enable all Secondary CWMGateway processes to detect whenever the Primary CWMGateway dies unexpectedly and vice versa. Loss of a heartbeat message from the Primary CWMGateway in two consecutive heartbeat intervals will indicate a loss of IP connectivity.

Note An *Abnormal Exit* happens when a CWM Gateway process is stopped through a non-graceful shutdown. This includes when a process has been stopped with a **process core dump** command, but does not include a power down.

Unexpected Exit of the Primary CWMGateway

The unexpected exit of the Primary CWMGateway will be detected by the Secondary CWMGateway through the Orbix callback (CORBA::IT_IOCallback) mechanism, which is invoked when the CORBA connection between them is broken (provided that there is IP connectivity between the Primary and the Secondary). The CWMGateway process will automatically be restarted by *watchdog* up to 5 times. Once the Primary is restarted it will notify all Secondaries. Upon receiving this event, a Secondary CWMGateway will re-register with the Primary.

If all Secondaries did not receive notification of the Primary restart either due to the Primary CWM's failure to restart after five attempts, or because IP connectivity was lost between the Secondary and the Primary, the Secondaries will continue to work as Secondaries with no Primary CWM present, in a degraded mode of operation.

Unexpected Exit of the Secondary CWMGateway

The unexpected exit of a Secondary CWMGateway will be detected by the Primary CWMGateway through the Orbix callback (CORBA::IT_IOCallback) mechanism. The Primary CWMGateway will reassign the priority (decremented by 1) of all Secondary CWMGateways whose priority number was higher than the priority number of the departed Secondary, and will remove the client entry corresponding to this Secondary CWMGateway from its list.

Primary CWM has lost IP or physical connectivity to all Secondary CWMs

- To recover from this degraded mode of operation, re-establish IP connectivity on the Primary CWM and then all Secondary CWMs will automatically re-sync their user data tables with the Primary CWM.
- **If you can't re-establish IP connectivity on the Primary**, then eliminate the downed Primary from the CWM domain by following these steps:

Step 1 Manually remove the downed Primary from all the other CWM's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of a **CWMGateway.conf file** with a **DomainGatewayList** consisting of three CWM workstations named cwmws1, cwmws2, and cwmws3, with cwmws1 assigned as the Primary and cwmws2 and cwmws3 assigned as Secondaries:

```
Debug level 2
DomainGatewayList cwmws1 cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

The above **DomainGatewayList, for example,** would need to be edited to show that the downed Primary (cwmws1) has been removed from all the other CWM's **DomainGatewayLists** in the **CWMGateway.conf** file. In this example, you would remove the downed Primary from both cwmws2 and cwmws3 **DomainGatewayLists** to include only cwmws2 and cwmws3 Secondaries in the same domain:

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 2 Manually remove all the other CWMs from the downed Primary's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of the downed Primary's **DomainGatewayList**. Remove all Secondary CWMs from the downed Primary's **DomainGatewayList** leaving the Primary cwmws1 in its own domain:

```
Debug level 2
DomainGatewayList cwmws1
ForcedSwitchOver
HeartBeatInterval 20
```

Step 3 Stop the core on the downed Primary CWM. (This is done to eliminate the possibility of having two Primary CWMs running at the same time once IP connectivity has been re-established. The isolated Primary CWM needs to be kept from communicating with CWMs in its old domain, which will have a newly assigned Primary CWM and Secondary CWMs. Once IP connectivity has been re-established, the original Primary will have to be added back to the domain by editing it and the other CWM's **DomainGatewayList**).

Step 4 Stop the core on the Secondary CWM that has been selected as the new Primary. In this case, for example, let's say that cwmws2 has been selected as the new Primary.

Step 5 Edit the new Primary's **DomainGatewayList so that it only has itself listed. For example:**

```
Debug level 2
DomainGatewayList cwmws2
ForcedSwitchOver
HeartBeatInterval 20
```

Step 6 Start the core on the new Primary CWM (in this example it would be cwmws2). A message will appear on the CWM console announcing it as the new Primary.

Step 7 Stop the core on the Secondary CWM (in this example it would be cwmws3).

Step 8 Edit the Secondary's **DomainGatewayList so that it includes itself and the new Primary. For example:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 9 Edit the new Primary's **DomainGatewayList so that it now includes itself and the secondary CWM. For example:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 10 Start the core on the Secondary CWM (in this example it would be cwmws3).

Step 11 Repeat steps 7-10 above to include any additional Secondary CWMs in the new domain. The **DomainGatewayList on all of the Secondary CWMs must match the final DomainGatewayList on the Primary CWM. This list will include the new Primary and all new Secondaries in the new domain.**

One Secondary CWM has lost IP connectivity with the Primary CWM

– To recover from this degraded mode of operation, re-establish IP connectivity on the Secondary CWM, and the Secondary CWM will automatically re-sync the user data tables with the Primary CWM.

Note IP Connectivity is still maintained between the Primary CWM and the other Secondary CWMs in this scenario. Only the Secondary CWM that has lost IP connectivity with the Primary CWM will be working in the degrade mode until its IP connectivity is re-established.

The CWM Gateway process dies on the Primary and is NOT restarted by *watchdog*

– To recover from this degraded mode of operation, warm start *only* on the Primary CWM. In this case the original Primary CWM is still the designated Primary CWM, and the Secondary CWMs automatically re-sync user data tables.

Note User data provisioning is still in progress on the Primary CWM without the CWM Gateway process running. Additionally, in this case, the Primary CWM still has connectivity with all Secondary CWMs.

– **If a Warm start does not work**, then eliminate the downed Primary from the CWM domain by following these steps:

Step 1 Manually remove the downed Primary from all the other CWM's **DomainGatewayLists** in the **CWMGateway.conf** file

The following is an example of a **CWMGateway.conf file** with a **DomainGatewayList** consisting of three CWM workstations named cwmws1, cwmws2, and cwmws3, with cwmws1 assigned as the Primary and cwmws2 and cwmws3 assigned as Secondaries:

```
Debug level 2
DomainGatewayList cwmws1 cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

The above **DomainGatewayList, for example,** would need to be edited to show that the downed Primary has been removed from all the other CWM's **DomainGatewayLists** in the **CWMGateway.conf** file. In this example, you would remove the downed Primary from both cwmws2 and cwmws3 **DomainGatewayLists** to include only cwmws2 and cwmws3 Secondaries in the same domain:

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
```

```
ForcedSwitchOver
HeartBeatInterval 20
```

Step 2 Manually remove all the other CWMs from the downed Primary's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of the downed Primary's **DomainGatewayList**. Remove all Secondary CWMs from the downed Primary's **DomainGatewayList** leaving the Primary cwmws1 in its own domain:

```
Debug level 2
DomainGatewayList cwmws1
ForcedSwitchOver
HeartBeatInterval 20
```

Step 3 Stop the core on the downed Primary CWM. (This is an optional step).

Step 4 Stop the core on the Secondary CWM that has been selected as the new Primary. In this case, for example, let's say that cwmws2 has been selected as the new Primary.

Step 5 Edit the new Primary's **DomainGatewayList so that it only has itself listed. For example:**

```
Debug level 2
DomainGatewayList cwmws2
ForcedSwitchOver
HeartBeatInterval 20
```

Step 6 To ensure a manual re-sync of user data tables between the downed Primary CWM and the newly assigned Primary CWM, enter **usrtblDBsync** <**cwmws1**> (with "cwmws1" representing the original Primary CWM).

Step 7 Start the core on the new Primary CWM (in this example it would be cwmws2). A message will appear on the CWM console announcing it as the new Primary.

Step 8 Stop the core on the Secondary CWM (in this example it would be cwmws3).

Step 9 Edit the Secondary's **DomainGatewayList so that it includes itself and the new Primary. For example:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 10 Edit the new Primary's **DomainGatewayList so that it now includes itself and the secondary CWM. For example:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 11 Start the core on the Secondary CWM (in this example it would be cwmws3).

Step 12 Repeat steps 7-10 above to include any additional Secondary CWMs in the new domain. The **DomainGatewayList on all of the Secondary CWMs must match the final DomainGatewayList on the Primary CWM. This list will include the new Primary and all new Secondaries in the new domain.**

The CWM Workstation Crashed or was Powered-off (Disaster Recovery)

Note A CWM W/S crash includes a power down, power failure, or disk crash.

– To recover from this degraded mode of operation follow these steps:

Step 1 Use the kill command (**-9**) on the CWMGateway process on the Secondary CWMs, after a successful re-start of the Primary CWM.

Step 2 The CWMGateway process will then be re-started by Watchdog within seconds.

Step 3 Manually re-sync the user data tables with the **usertblDBsync c**ommand. Or, avoid doing any new user data provisioning on the re-started Primary CWM until all of the Secondary CWMs are out of degrade mode.

– An alternate approach to re-starting the Primary CWM is as follows:

Step 1 Start the core on the Primary

Step 2 Stop the core on all Secondaries

Step 3 Start the core on the Secondary CWMs in the network one by one.

– Eliminate the downed Primary from the CWM domain **only if power-on or re-start of the Primary does not work** by following these steps:

Step 1 Manually remove the downed Primary from all the other CWM's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of a **CWMGateway.conf file** with a **DomainGatewayList** consisting of three CWM workstations named cwmws1, cwmws2, and cwmws3, with cwmws1 assigned as the Primary and cwmws2 and cwmws3 assigned as Secondaries:

```
Debug level 2
DomainGatewayList cwmws1 cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

The above **DomainGatewayList, for example,** would need to be edited to show that the downed Primary has been removed from all the other CWM's **DomainGatewayLists** in the **CWMGateway.conf** file. In this example, you would remove the downed Primary from both cwmws2 and cwmws3 **DomainGatewayLists** to include only cwmws2 and cwmws3 Secondaries in the same domain:

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 2 Manually remove all the other CWMs from the downed Primary's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of the downed Primary's **DomainGatewayList**. Remove all Secondary CWMs from the downed Primary's **DomainGatewayList** leaving the Primary cwmws1 in its own domain:

```
Debug level 2
DomainGatewayList cwmws1
ForcedSwitchOver
HeartBeatInterval 20
```

Step 3 Stop the core on the downed Primary CWM (to prevent communication with the Secondary CWMs while the Primary is down and isolated).

Step 4 Stop the core on the Secondary CWM that has been selected as the new Primary. In this case, for example, let's say that cwmws2 has been selected as the new Primary.

Step 5 Edit the new Primary's **DomainGatewayList so that it only has itself listed. For example:**

```
Debug level 2
DomainGatewayList cwmws2
ForcedSwitchOver
HeartBeatInterval 20
```

Step 6 Start the core on the new Primary CWM (in this example it would be cwmws2). A message will appear on the CWM console announcing it as the new Primary.

Step 7 Stop the core on the Secondary CWM (in this example it would be cwmws3).

Step 8 Edit the Secondary's **DomainGatewayList so that it includes itself and the new Primary. For example:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 9 Edit the new Primary's **DomainGatewayList so that it now includes itself and the secondary CWM. For example:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 10 Start the core on the Secondary CWM (in this example it would be cwmws3).

Step 11 Repeat steps 7-10 above to include any additional Secondary CWMs in the new domain. The **DomainGatewayList on all of the Secondary CWMs must match the final DomainGatewayList on the Primary CWM. This list will include the new Primary and all new Secondaries in the new domain.**

The Primary CWM has lost IP or physical connectivity with the only Secondary CWM in a domain

Note In a situation where there is a Primary CWM and only one Secondary CWM in a given domain, and connectivity between the two CWMs is lost, another Secondary CWM will need to be added to the domain before stopping the core on the original Secondary CWM.

– To recover from this degraded mode of operation, re-establish IP connectivity on the Primary CWM and the Secondary CWM will automatically re-sync user data tables with the Primary CWM.

– **If you can't re-establish IP connectivity on the Primary**, then eliminate the downed Primary from the CWM domain by following these steps:

Step 1 Manually remove the downed Primary from the Secondary CWM's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of a **CWMGateway.conf file** with a **DomainGatewayList** consisting of two CWM workstations named cwmws1 and cwmws2, with cwmws1 assigned as the Primary and cwmws2 as the Secondary:

```
Debug level 2
DomainGatewayList cwmws1 cwmws2
ForcedSwitchOver
HeartBeatInterval 20
```

The above **DomainGatewayList, for example,** would need to be edited to show that the downed Primary (cwmws1) has been removed from the Secondary CWM's (cwmws2) **DomainGatewayList** in the **CWMGateway.conf** file. In this example, you would remove the downed Primary from the cwmws2 **DomainGatewayList** to include only cwmws2:

```
Debug level 2
DomainGatewayList cwmws2
ForcedSwitchOver
HeartBeatInterval 20
```

Step 2 Manually remove the Secondary CWM (cwmws2) from the downed Primary's **DomainGatewayList** in the **CWMGateway.conf** file

The following is an example of the downed Primary's **DomainGatewayList after removing** the Secondary CWM from the downed Primary's **DomainGatewayList,** leaving the Primary cwmws1 in its own domain:

```
Debug level 2
DomainGatewayList cwmws1
ForcedSwitchOver
HeartBeatInterval 20
```

Step 3 Stop the core on the downed Primary CWM.

Step 4 Start the core on the downed Primary CWM (this is an optional step).

Step 5 Add another workstation (for example, cwmws3) to serve as the new Primary CWM. Install CWM on this workstation if it is not already installed, or **cold start -F** if CWM is already installed on this new workstation.

Note Do not **cold start -F** without first verifying that a Secondary CWM has switched over to become the new Primary CWM of the domain, otherwise the node_id and other user data will become inconsistent.

Step 6 To ensure a manual re-sync of user data tables between the original Secondary CWM and a new Primary CWM, enter **usrtblDBsync** <**cwmws3**> on the new Primary CWM.

Step 7 Edit the new Primary's **DomainGatewayList so that it includes itself. For example, let's say that a new Primary CWM named cwmws3 has been brought into the domain, its DomainGatewayList would look like this:**

```
Debug level 2
DomainGatewayList cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 8 Start the core on the new Primary CWM (in this example it would be cwmws3).

Step 9 Stop the core on the original Secondary CWM (in this example it would be cwmws2).

Step 10 Edit the original Secondary CWM's **DomainGatewayList so that it includes itself and the new Primary CWM. For example, its DomainGatewayList would look like this:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 11 Edit the new Primary CWM's **DomainGatewayList so that it includes itself and the original Secondary CWM. For example, its DomainGatewayList would look like this:**

```
Debug level 2
DomainGatewayList cwmws2 cwmws3
ForcedSwitchOver
HeartBeatInterval 20
```

Step 12 Start the core on the original Secondary CWM (in this example it would be cwmws2).

Loss of Heartbeat from Primary CWMGateway

A Secondary CWMGateway will consider itself disconnected from the Primary, and in a degraded mode of operation, if it fails to receive a heartbeat message during two successive heartbeat intervals. There will be no switchover in this situation. The Secondary CWMGateway will log an L1 message and a print error message on the console indicating that it has lost connectivity to the Primary CWMGateway. This will be repeated every 60 seconds. It will go back to the normal mode of operation once the heartbeat message has been received. The Secondary CWMGateway will work in a degraded mode of operation until, and unless, the heartbeat is restored from the Primary.

Note The Secondary CWMs will receive heartbeat messages from the Primary CWM as soon as the connection has been re-established, if either end (Primary or SecondaryGateway) is restarted, or if the problem for an existing connection has been resolved (i.e. change a broken network cable). There is no dependency between sending heartbeat messages from the Primary CWM to the Secondary CWM, and CWM sync-up with the managed network.

Review of Warm and Cold Start of CWM

Performing a Warm Start of CWM

A warm start of CWM consists of stopping the application, then restarting it. A warm start of CWM is used without initializing the database, and can aid in overcoming database inconsistencies without losing data. **When you perform a warm start of CWM, the application continues to use data in the existing Informix database**.

To perform a warm start of CWM, complete the following steps:

Step 1 From the CWM main menu, enter **2** to select the **Stop Core** option, then confirm that you want to stop core by responding **y** to the prompt.

It should take less than a minute for all of the processes and messages to end.

Step 2 Press Return to re-display the CWM main menu.

Step 3 From the main menu, enter **1** to select the Start Core option.

Step 4 When the CWM main menu is displayed, enter **3** to launch the CWM Desktop.

Performing a Cold Start of CWM

You perform a cold start of CWM when starting the application with an empty database. A cold start is typically used following a CWM upgrade or if there were too many database inconsistencies within the network for a warm start recovery to be successful. You can use the **create_db, or coldstart -F or Sv+CreateDb -F** commands to build a new, empty database. These commands **destroy any existing data in the database including statistics and object comments**.

Note The user needs to run **updateftpinfo** after a **coldstart -F**, or after a change has been made to their UNIX password of svplus after installation.

Note In any degrade mode recovery procedure, the user data tables should be kept on the Primary CWM in order to maintain all existing user data. This means that the user should not use **coldstart -F** or **SV+CreateDB -F** on the Primary CWM or all of the existing user data will be dropped from the database. Similar commands, **SV+CreateDB** or **coldstart**, can be used on the Primary CWM to clear all of the network data, and as soon as a connection has been re-established, the Secondary CWM will re-sync the user data tables with the Primary CWM.

To perform a cold start of CWM, complete the following steps:

Step 1 At the CWM workstation, enter **CWM** to display the main menu.

Step 2 From the CWM main menu, enter **2** to select the **Stop Core** option, then confirm that you want to stop core by responding **y** to the prompt.

It might take several minutes for all of the processes and messages to end, depending upon the number of nodes in the network.

Step 3 Press Return to redisplay the CWM main menu.

Step 4 From the main menu, enter **x** to exit the CWM application.

Step 5 Enter **create_db, or coldstart -F or Sv+CreateDb -F**.

Dozens of messages will be displayed, starting with the message **dropping db**. Additional messages will indicate that tables are being created and procedures stored. The shell prompt will return in less than a minute.

Step 6 At the CWM workstation, enter **CWM** to redisplay the main menu.

Step 7 From the main menu, enter **1** to select the Start Core option.

Step 8 When the CWM main menu is displayed, enter **3** to launch the CWM Desktop.

Limitations for CWM to CWM Communications

- The Secondary CWMs have to wait for the Primary CWM to finish syncing up with the network. Trap 28075 (svDatabaseInSync) is sent when the Primary CWM has finished syncing up with the network.
- All the CWM workstations managing the same network must have seed nodes or gateway nodes that have IP addresses within the same domain.

Note The **network.conf** file does not have to be the same on all CWM stations in the domain as long as the gateway nodes specified in this file are part of the same network. Even though CWMs that manage the same network can talk to each other, managing the same network does not require having identical **network.conf** files on all Secondary and Primary CWMs.

- The Configurator can only be run on the Primary CWM.
- If all the Secondary CWM Gateways lose IP connection with the Primary CWM Gateway (no heartbeat received in the past 2 consecutive Heartbeat Intervals), then all the Secondary CWM Gateways will function in degraded mode and wait for the connection problem to be resolved.

Note Do not **cold start -F** without first verifying that a Secondary CWM has switched over to become the new Primary CWM of the domain, otherwise the node_id and other user data will become inconsistent.

Enabling CWM to CWM Communications

In Release 10.5, CWM provides a script to sync up a CWM database with another remote CWM workstation without running the two CWMs in primary-secondary mode.

The script synchronizes the following user-related tables in the stratacom database:

- node_info
- user_info
- sec_profile
- xpvc_preferred
- xpvc
- xpvc_segment
- sct
- sct_cosb
- sct_vc
- sct_usage
- conn_template
- conn_templ_param
- scmcardenable
- scmnodeenable
- scmnodecollhost
- scmtemplate
- scmcolpar
- scmcolparsubobj
- scmcolparstat
- user_conn_desc

Note The script will delete whatever existing data is in the tables on the local workstation. Do not expect to retain any existing data in the tables after running the script.

Steps for Executing the usertblDBsync and usertblDBcmp Scripts

Execute the following steps to *copy* the remote table containing user data information to the database on the local machine by running the **usertblDBsync** script.

Step 1 Execute the **usertblDBsync** script

% usertblDBsync <remote_CWM_workstation_name>

Example:

mmen% **usertblDBsync mmenu10**

Note This will destroy all the data in the following tables from the local CWM Database and load the data from CWM on host mmenu10.

- + node_info
- + user_info

- + sec_profile
- + xpvc_preferred
- + xpvc
- + xpvc_segment
- + sct
- + sct_cosb
- + sct_vc
- + sct_usage
- + conn_template
- + conn_templ_param
- + scmcardenable
- + scmnodeenable
- + scmnodecollhost
- + scmtemplate
- + scmcolpar
- + scmcolparsubobj
- + scmcolparstat
- + user_conn_desc

Continue to sync? [No]**y**

**********Syncing user tables with CWM on host [cwmtopo62]**********

Syncing Table node_info@mmendsl2 with

node_info@cwmtopo62.....[DONE]

Syncing Table user_info@mmendsl2 with

user_info@cwmtopo62.....[DONE]

Syncing Table sec_profile@mmendsl2 with

sec_profile@cwmtopo62.....[DONE]

Syncing Table xpvc_preferred@mmendsl2 with

xpvc_preferred@cwmtopo62.....[DONE]

Syncing Table xpvc@mmendsl2 with

xpvc@cwmtopo62.....[DONE]

Syncing Table xpvc_segment@mmendsl2 with

xpvc_segment@cwmtopo62.....[DONE]

Syncing Table sct@mmendsl2 with

sct@cwmtopo62.....[DONE]

Syncing Table sct_cosb@mmendsl2 with

sct_cosb@cwmtopo62.....[DONE]

Syncing Table sct_vc@mmendsl2 with

sct_vc@cwmtopo62.....[DONE]

```
Syncing Table sct_usage@mmendsl2 with
sct_usage@cwmtopo62.....[DONE]
Syncing Table conn_template@mmendsl2 with
conn_template@cwmtopo62.....[DONE]
Syncing Table conn_templ_param@mmendsl2 with
conn_templ_param@cwmtopo62.....[DONE]
Syncing Table scmcardenable@mmendsl2 with
scmcardenable@cwmtopo62.....[DONE]
Syncing Table scmnodeenable@mmendsl2 with
scmnodeenable@cwmtopo62.....[DONE]
Syncing Table scmnodecollhost@mmendsl2 with
scmnodecollhost@cwmtopo62.....[DONE]
Syncing Table scmtemplate@mmendsl2 with
scmtemplate@cwmtopo62.....[DONE]
Syncing Table scmcolpar@mmendsl2 with
scmcolpar@cwmtopo62.....[DONE]
Syncing Table scmcolparsubobj@mmendsl2 with
scmcolparsubobj@cwmtopo62.....[DONE]
Syncing Table scmcolparstat@mmendsl2 with
scmcolparstat@cwmtopo62.....[DONE]
Syncing Table user_conn_desc@mmendsl2 with
user_conn_desc@cwmtopo62.....[DONE]
mmendsl2-11->
```

Executing this script copies the following user-related tables in the stratacom database from the remote CWM workstation specified by <*remote_CWM_workstation_name*> to the local machine:

- node_info
- user_info
- sec_profile
- xpvc_preferred
- xpvc
- xpvc_segment
- sct
- sct_cosb
- sct_vc
- sct_usage
- conn_template
- conn_templ_param
- scmcardenable

- scmnodeenable
- scmnodecollhost
- scmtemplate
- scmcolpar
- scmcolparsubobj
- scmcolparstat
- user_conn_desc

Note Ensure that the networks in the network.conf file on the local machine are the same as those specified in the network.conf file on the remote CWM station, where CWM is already synced up. You will see a warning to this effect displayed on the screen after the tables have been successfully loaded.

Execute the following steps to *compare* the remote table containing user data information to the database on the local machine by running the **usertblDBcmp** script.

Step 1 Execute the **usertblDBcmp** script

% usertblDBcmp <remote_CWM_workstation_name>

Example:

mmen% **usertblDBcmp mmenu10**

- + node_info
- + user_info
- + sec_profile
- + xpvc_preferred
- + xpvc
- + xpvc_segment
- + sct
- + sct_cosb
- + sct_vc
- + sct_usage
- + conn_template
- + conn_templ_param
- + scmcardenable
- + scmnodeenable
- + scmnodecollhost
- + scmtemplate
- + scmcolpar
- + scmcolparsubobj

- + scmcolparstat
- + user_conn_desc

```
cwmtopo62-10-> usertblDBcmp mmen
**********Comparing user tables with CWM on host [mmen]**********
Comparing Table node_info@cwmtopo62 with
node_info@mmen.....[SAME]
Comparing Table user_info@cwmtopo62 with
user_info@mmen.....[SAME]
Comparing Table sec_profile@cwmtopo62 with
sec_profile@mmen.....[SAME]
Comparing Table xpvc_preferred@cwmtopo62 with
xpvc_preferred@mmen.....[SAME]
Comparing Table xpvc@cwmtopo62 with
xpvc@mmen.....[SAME]
Comparing Table xpvc_segment@cwmtopo62 with
xpvc_segment@mmen.....[SAME]
Comparing Table sct@cwmtopo62 with
sct@mmen.....[SAME]
Comparing Table sct_cosb@cwmtopo62 with
sct_cosb@mmen.....[SAME]
Comparing Table sct_vc@cwmtopo62 with
sct_vc@mmen.....[SAME]
Comparing Table sct_usage@cwmtopo62 with
sct_usage@mmen.....[SAME]
Comparing Table conn_template@cwmtopo62 with
conn_template@mmen.....[SAME]
Comparing Table conn_templ_param@cwmtopo62 with
conn_templ_param@mmen.....[SAME]
Comparing Table scmcardenable@cwmtopo62 with
scmcardenable@mmen.....[SAME]
Comparing Table scmnodeenable@cwmtopo62 with
scmnodeenable@mmen.....[SAME]
Comparing Table scmnodecollhost@cwmtopo62 with
scmnodecollhost@mmen.....[SAME]
Comparing Table scmtemplate@cwmtopo62 with
scmtemplate@mmen.....[SAME]
Comparing Table scmcolpar@cwmtopo62 with
scmcolpar@mmen.....[SAME]
```

Comparing Table scmcolparsubobj@cwmtopo62 with scmcolparsubobj@mmen.....[SAME]
Comparing Table scmcolparstat@cwmtopo62 with scmcolparstat@mmen.....[SAME]
Comparing Table user_conn_desc@cwmtopo62 with user_conn_desc@mmen.....[SAME]
cwmtopo62-10->

CHAPTER 12

Downloading Software and Firmware

Introduction

This chapter provides information for downloading software and firmware, describes where to obtain it, and details the required preparations and procedures for downloading software and firmware from the CWM workstation to a Cisco WAN switch.

The TFTP/FTP protocol is used to download software and firmware images from the CWM workstation to WAN switches.

Note A CWM workstation is not required to download the software images. You can download the software images using any machine that can run a FTP client/server process.

Note CWM Image Download *only* transfers the image file from the CWM workstation to the switch.

Where to Get Switch Images for Downloading

Cisco Connection Online (CCO) provides a web page, **WAN Switching Upgrade Planner**, that provides information about the latest Cisco software product. If you have a Cisco Connection Online account, you can order or download software directly to your system. The URL for CCO software and firmware is:

http://www.cisco.com/kobayashi/sw-center/wan/wan-planner.shtml

The WAN Switching Upgrade Planner web page provides links to the following:

- Product Information for WAN Switching Products
- Release Information for WAN Switching Products
- Documentation and Release Notes
- Older Software for WAN Switching Products
- Download Cisco WAN Switching Software
- Download Cisco WAN Card Firmware

Preparing the IPX/BPX Switch to Download Software or Firmware

Before downloading software and firmware to a switch, use the Switch CLI (Command Line Interface) to execute the following commands. This is required regardless of how the software image transfer will be initiated.

Note The following procedures are applicable to IPX and BPX switches only.

Step 1 Access the Switch CLI by attaching a dumb terminal to the switch or **telnet** to the switch.

When you select the switch node from the CWM Network Topology window and then select the **Node** menu's **Node Admin** option, the CWM software telnets to the switch. A new terminal window is displayed for your use.

Step 2 Enable the switch to allow downloading. From the Switch CLI, execute the following command: **cnffunc**

Step 3 Use the **Index** column's value for the **Download From Remote StrataView** entry in the following command:

cnffunc <*index*> **e**

In the example, <*index*> would be set to **6**. The "**e**" parameter specifies to enable the function. Once this command is executed, the switch allows downloading from a CWM workstation, provided the latter is connected to another switch in the same network.

Step 4 Invoke the following command when a redundant processor card is not installed.

cnfnodeparm

shows sample output from the **cnfnodeparm** command. When a redundant processor card (BCC, NPM, or NPC) is not installed, you should set the parameter indicating the presence of a redundant processor to **No**. In the command output, look for the number corresponding to the **CC Redundancy Cnfged** entry.

Step 5 Invoke the following command:

cnfnodeparm <*number*> **N**

When you have a redundant processor card and the value for the parameter **CC Redundancy Cnfged** is **Yes,** you are requesting an image download into both processors (active and redundant).

Note If **CC Redundancy Cnfged** is Yes and no redundant processor card is present, the download is suspended.

Step 6 Configure the switch to receive software or firmware images from the CWM workstation by invoking the **cnffwswinit** command:

cnffwswinit <*IP_addr_CWM_workstation*>

Note The step above is required if you are using a CWM workstation to send the download request to the switch.

Downloading Switch Software or Firmware From the CWM Workstation to a Switch

To download images to an MGX, complete the following steps:

Step 1 Copy IPX or BPX images to the CWM workstation's **/usr/users/svplus/images/ipxbpx** directory, and MGX images to the **/usr/users/svplus/images/mgx** directory.

Step 2 Launch the CWM desktop and login as a user with All access privileges for Topology. The Network Topology window is displayed.

Step 3 Click on the node icon in the Network Topology window, upon which you want to download the switch software/firmware images, then select **SW/FW Images** from the **Tools** dropdown menu of the Topology menu bar.

The Image DownLoader window is displayed. This window displays a list of the software that is loaded on the CWM workstation (in the **/usr/users/svplus/images/** directory) for the type of node selected.Choose the image you wish to download, then select **Download**.

When the download has completed, please telnet to the switch and use the switch CLI to verify and invoke the images.

Note For additional details pertaining to the switches, please refer to the appropriate Cisco switch documentation.

Image Filename Conventions

The following naming conventions are used for software images:

IGX and BPX Conventions

IGX and BPX software images have the following format (where Release is 9.2.0):

```
<Release>.img
<9.2.0>.img
<9.2.0>.000
...
<9.2.0>.022
```

IGX and BPX firmware images have the following format:

```
<FW Release>.img
<A.A.02>.img
```

MGX Conventions

The following naming convention is used for software images:

*<cardtype>*_<*A*>_<*B*> [<*C*>_<*D*>]**.fw**

where <*cardtype*> is a name of the card. <*A*>, <*B*>, <*C*>, and <*D*> can be a string containing any combination of numerals and characters. <A>_<B> <C>_<D> indicates the firmware version number of a given image file. <C> and <D> are optional. The **.fw** extension indicates the file is a firmware image.

Monitoring a Download Session on BPX and IGX Nodes

The commands **dsprev** (software) and **dspfwrevs** (firmware) display existing software (or firmware) revisions on a routing network, as well as the revisions currently being downloaded. When these commands are issued at a feeder, revisions on that feeder alone appear on the screen.

You can use the **dsprev** or **dspfwrevs** commands to see when downloading of the software or firmware is complete.

CHAPTER 13

Saving and Restoring Node Configurations

Release 10 of CWM **ConfigSave and Restore** is a new Java-based application that is launched from the desktop. Select **Tools** from the main menu bar of the Network Topology window, and then click the **ConfigSave and Restore** submenu to launch the **ConfigSave and Restore application.**

The following node platforms are supported by the new ConfigSave and Restore application:

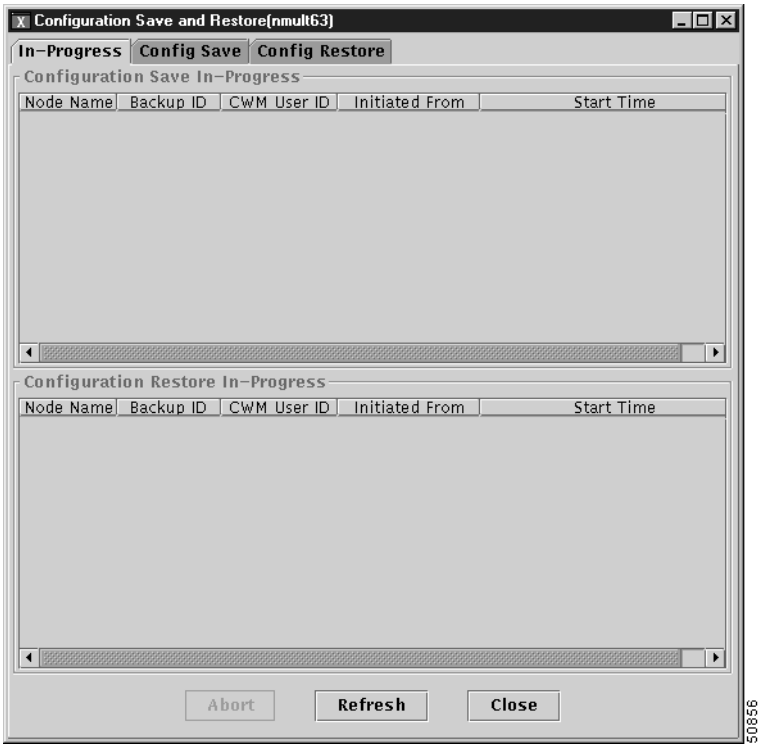
MGX 8220 (AXIS), BPX 8600, MGX 8850 PXM1, MGX 8850 PXM 45, IGX, BPX-SES, MGX 8230, and MGX 8250.

Note This new Java version of CWM ConfigSave and Restore does not support HP OpenView.

Saving Node Configurations From CWM

This section describes how to save and restore node configurations. Figure 13-1 shows the **In Progress** window of the **ConfigSave and Restore** application where you can view Configuration Save in progress in the top panel of the screen, and Configuration Restore in progress in the bottom of the screen.

Figure 13-1 In Progress window

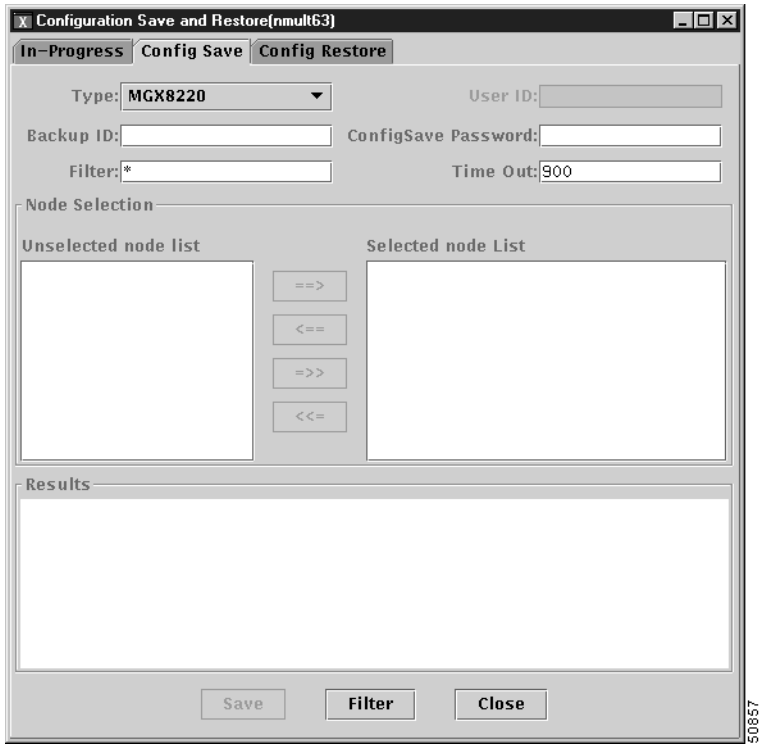


To save nodes, select the **Config Save** tab from the **ConfigSave and Restore main window as shown in** Figure 13-2. Enter all necessary fields and click the **Save** button. Results are displayed in the bottom panel of the screen; files will then be saved to the **usr/users/svplus/Config Data/<backup ID>_<node name>** directory.

Note Cisco has various restore commands for the different switching platforms.

You can also filter selections by clicking the **Filter** button at the bottom of the screen.

Figure 13-2 Configuration Save window



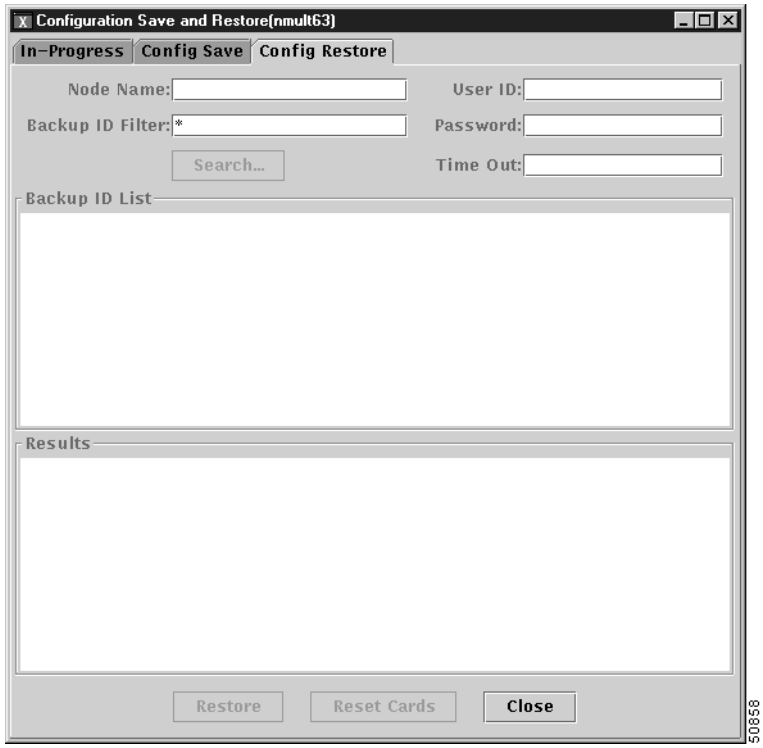
ConfigRestore from CWM

To restore configurations, select the **Config Restore** tab from the **ConfigSave and Restore main window as shown in** Figure 13-3. Enter all necessary fields and click the **Restore** button. Results are displayed in the bottom panel of the screen.

You can also reset cards by clicking the **Reset Cards** button at the bottom of the screen.

Note **The Reset Card option only applies to AXIS nodes.**

Figure 13-3 Configuration Restore window



Switch CLI Save and Restore

Release 10 of CWM **ConfigSave and Restore also allows saving and restoring of nodes through the Command Line Interface as follows:**

Saving Node Configurations for BPX and IGX Nodes

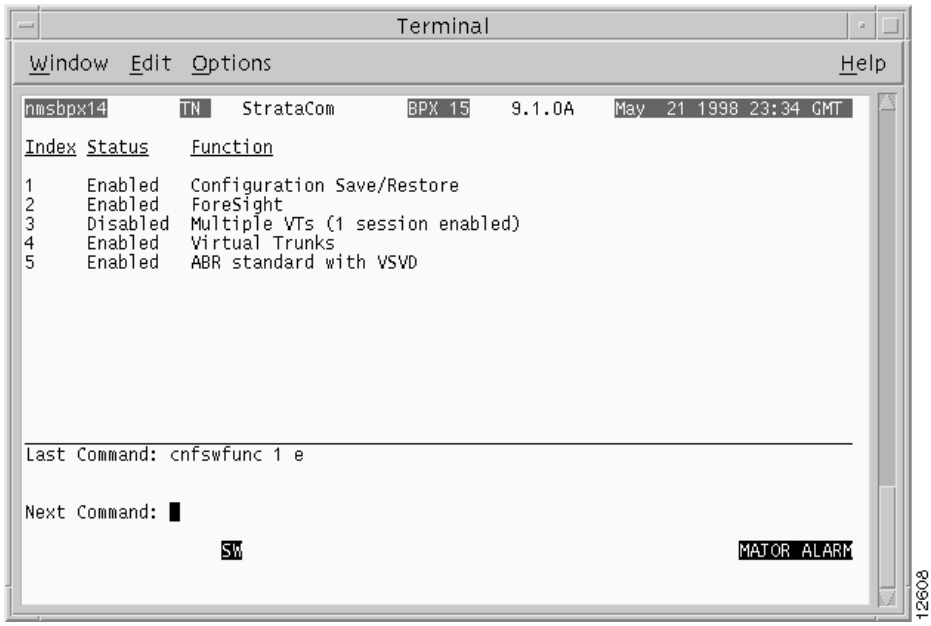
This section describes how to save and restore node configurations. To save or restore a node's configuration, the **Configuration Save/Restore** option should be enabled on the node.

Step 1 To enable or verify whether the **Configuration Save/Restore** option is enabled for a node, invoke the **cnfswfunc** command on the node CLI (Command Line Interface). The output of this command on a BPX 8600 is shown in Figure 13-4.

Note Step 1 is only used on BPX and IGX nodes.

Note The CWM ConfigSave and Restore feature must be enabled on the BPX and IGX nodes.

Figure 13-4 cnfswfunc Command Output



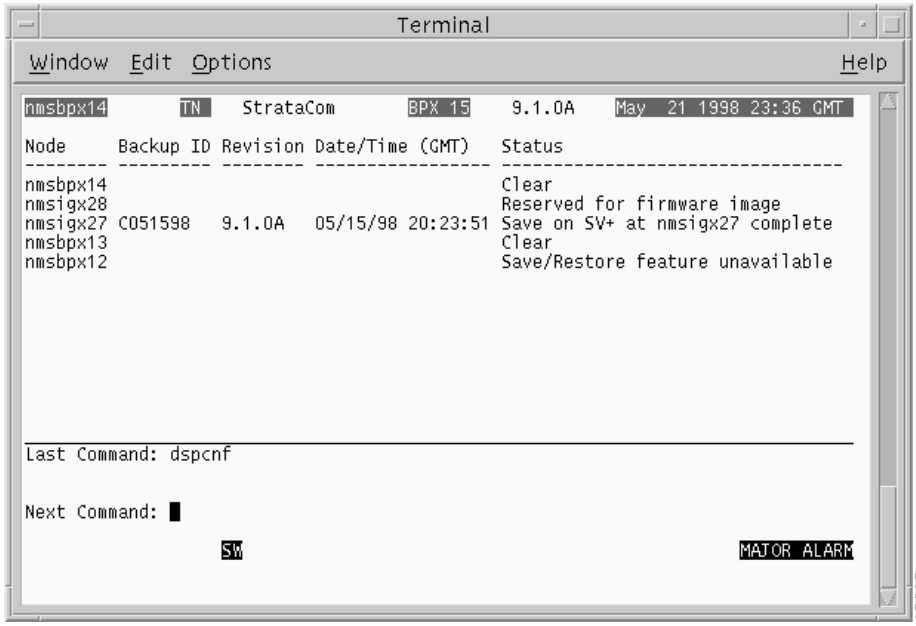
Option **1** in the above display is for Configuration Save and Restore. When this option is not enabled you can not save or restore the configuration from the node.

Note Note the output of **cnfswfunc** is different on an IGX 8400 series switch.

Step 2 Check whether a firmware image is loaded on the node. The **savecnf** command uses the same buffers used by a loaded firmware image. Therefore, when a firmware image is loaded on the node, **savecnf** displays an error. To check whether a firmware image is loaded on the node, invoke the **dspcnf** command. When the **dspcnf** output says “Reserved for firmware image” it means a firmware image is loaded on the node, as shown in Figure 13-5.

Note There are two prerequisites for BPX and IGX nodes: ConfigSave should be enabled, and the temporary memory should not be used by the firmware image.

Figure 13-5 dspcnf Command Output



Loaded firmware images must be cleaned up before invoking **savecnf**. To remove the loaded firmware image, invoke the **getfwrev** command on the node and specify **0.0** as the firmware revision level, as in the following:

getfwrev <card_type> 0.0 <node>

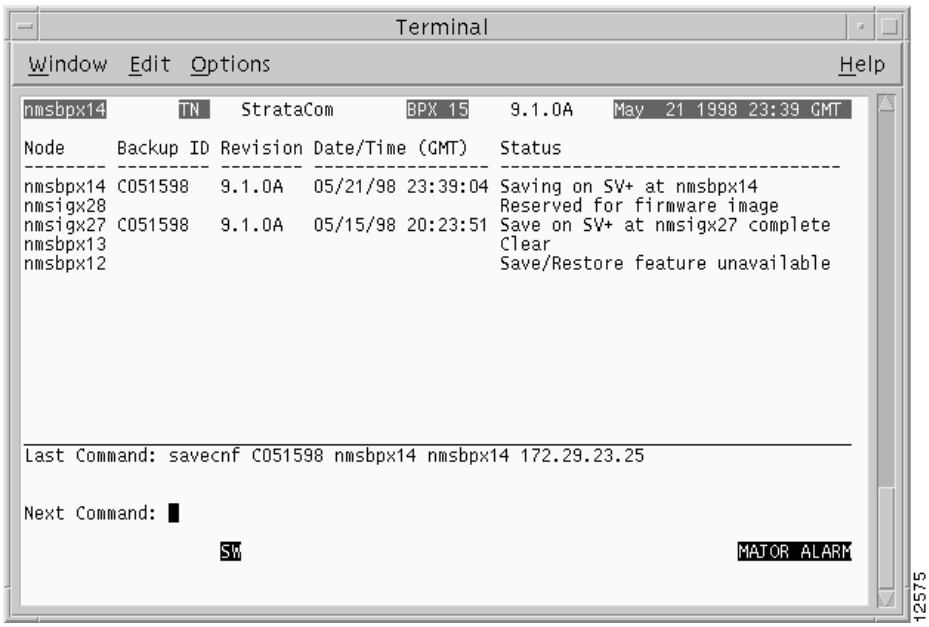
Step 3 Save the node's configuration using the **savecnf** command. The syntax for the **savecnf** command is given below:

savecnf <*backup_id*|*clear*> <*node_name*|*****> <*dest_SV_node*> [<*dest_SV_ip*>]

A typical **savecnf** command invocation is shown below with its output shown in Figure 13-6:

savecnf C051598 nmsbpx14 nmsbpx14 172.29.23.25

Figure 13-6 savecnf Command Output



When you specify an "*" (asterisk) as the third parameter to the **savecnf** command on a routing node, configuration of all the routing nodes in the network are saved. A directory with the name <*backup_id*>**_Cfgdir** is created in the home directory (**/usr/users/svplus**) of CWM and all the configuration files are saved in that directory.

When more than two CWM workstations are connected to the network, when you specify the last parameter (<*dest_SV_ip*>) you can identify to which CWM workstation the configuration save is to be done. In the above example, the configuration save is done on the CWM workstation with IP address **172.29.23.25**.

Note, the value for **dest_SV_node** is dependent on the configuration in **network.conf** file of CWM.

When the last field in a **/usr/users/svplus/network.conf** file entry is set to **nwip_on**, the **dest_SV_node** should be the same node on which the **savecnf** command is being executed. This case is shown in the typical invocation of the command, as shown above, where **dest_SV_node** is specified as **nmsbpx14** and the node on which **savecnf** is being run is also **nmsbpx14**.

Note You cannot invoke a save configuration of all nodes by specifying an "*****" (asterisk) as the third parameter to the **saveconf** command when **nwip_on** is configured in the **/usr/users/svplus/network.conf** file.

When the last field in a **/usr/users/svplus/network.conf** file entry is set to **nwip_off**, the **dest_SV_node** should be the gateway node name. Gateway node name is specified as the third field in a **/usr/users/svplus/network.conf** file entry of CWM. For example, the following command saves the configuration of node **nmsbpx14** on the CWM workstation, whose IP address is **172.29.23.25**, and is connected to the gateway node **nmsbpx13**.

savecnf C051598 nmsbpx14 nmsbpx13 172.29.23.25

To save the configuration of all routing nodes when **nwip_off** is configured in the **/usr/users/svplus/network.conf** file, a typical command invocation is:

savecnf C051598 * nmsbpx13 172.29.23.25

The above command saves the configuration of all routing nodes on the CWM workstation with the **172.29.23.25** IP address, and CWM gateway node specified as **nmsbpx13**. The configuration is saved in the **/usr/users/svplus/C051598_Cfgdir** directory.

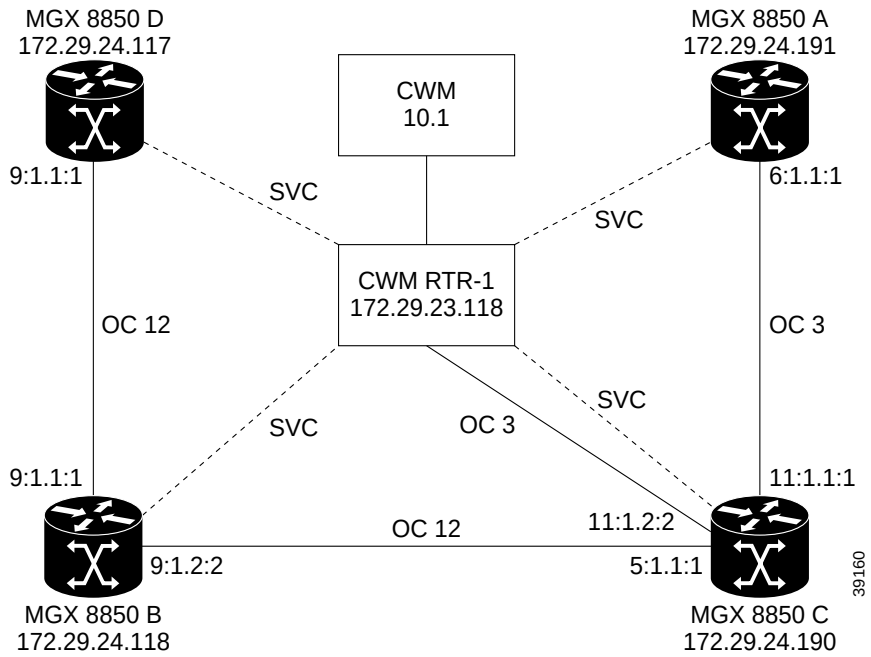
Restoring Node Configurations

To restore a node's configuration, invoke the **restorecnf** command. For the syntax of the **savecnf**, **restorecnf**, and other related commands, see the WAN Switching Super User Command Reference.

Internet Connectivity

This appendix provides information about how to achieve efficient internet connectivity for your Release 10 of CWM network management station for SVC connections and PNNI links. Figure A-1 shows a typical network configuration for a workstation running Release 10 of CWM.

Figure A-1 Typical Network Application



Overview

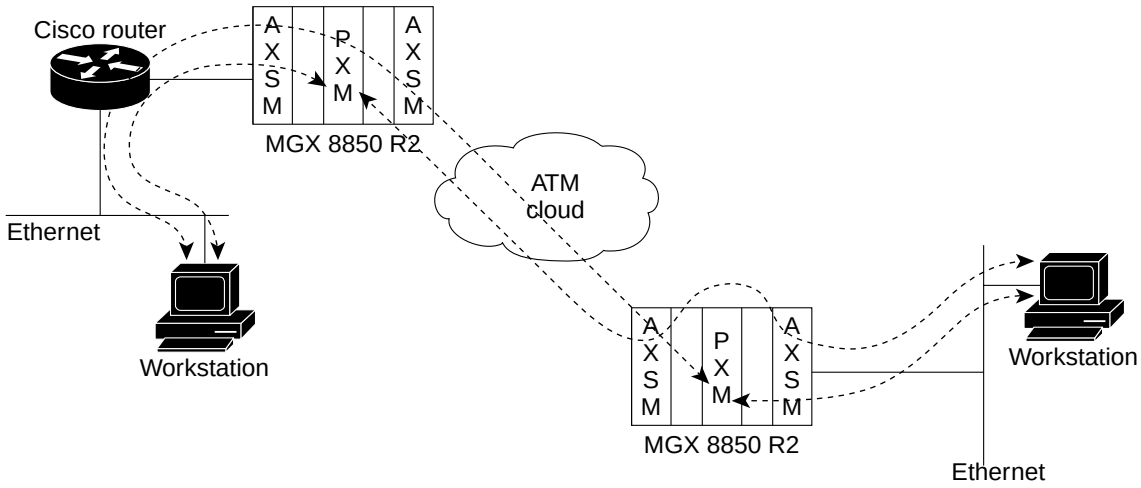
This section describes the IP Connectivity feature of the MGX 8850 Release 2. IP connectivity builds a IP data-path between a PXM and another IP host/workstation. Through IP connectivity, MGX 8850 Release 2 can be managed by a network management system such as CWM using standard TCP/IP and proprietary protocols.

The typical and most likely configuration will include the following:

- MGX 8850 Release 2 with external Cisco 7000 family or Cisco 4500 series router connected to AXSM port, or MGX 8850 Release 2 with internal RPM card to support Cisco 7200 router.
- Cisco router supports ATM interface with LLC encapsulation and ATMARP protocol service, RIP protocol and ILMI protocol.
- Host/workstation is a Sun workstation running Release 10 of CWM software with support for RIP and SNMP protocols.

Figure A-2 shows the logical connectivity between MGX 8850 Release 2 nodes and CWM workstations.

Figure A-2 MGX 8850 Release 2 IP Connectivity



Functional Description

IP connectivity relies on three disjoint IP hosts to build the IP data path. The first are the PXMs, where servers for the CWM, FTP, Telnet, etc. reside. The PXMs are the end-point for the MGX 8850 Release 2 being managed.

The second are router or routers. This routers interface with the PXMs using SVCs to transfer IP data. The routers will also interface with the CWM workstations that are managing the MGX 8850 Release 2 through some other network interface (usually ethernet).

The third are the CWM workstations managing the MGX 8850 Release 2. The CWM workstations initiate data being sent on the data-path to the MGX 8850 Release 2. The CWM workstation knows or learns that the routers are the go-between for all data to and from the MGX 8850 Release 2.

The CWM workstations will have clients such as CWM, FTP, Telnet, and TimeOfDay (among others) that will make IP connections with the appropriate servers on the MGX 8850 Release 2.

PXM

The PXM software provides for setting up the IP Connectivity data-path. This connectivity comes in several pieces. The first piece is the implementation of a custom interface for the VxWorks TCP/IP protocol stack. This custom interface will hook-up to the IP layer of the protocol stack and will have the

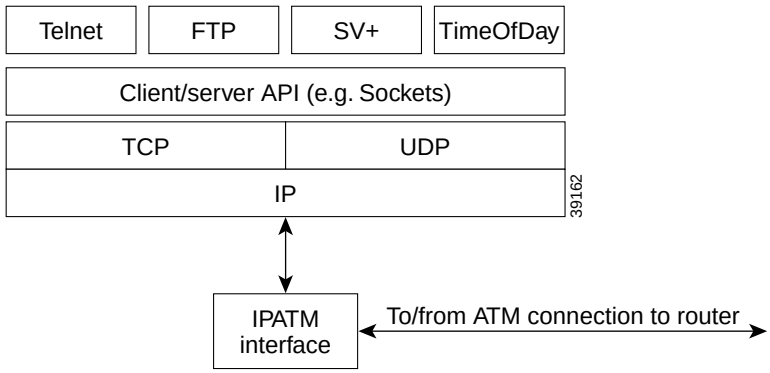
ability of transferring data between the ATM SAR and the IP stack. This custom interface will be assigned a unique IP address and will have the ability of creating and deleting IP host-routes that use the interface.

The custom interface will support IP over ATM as described in RFC1483. It will also be an ATMARP client as described by RFC1577. Figure A-3 shows the custom interface that for the remainder of this chapter will be referred to as the IPATM interface.

The IPATM requires the following configuration:

- IP address for the custom interface (address must be in same IP subnet as router)
- ATM End Station Address (AESA) to be used for SVC call requests to router
- Routers configured as AESA for router to be used by IPATM to connect SVC to router

Figure A-3 IPATM Custom Interface for VxWorks



IP Router

The IPATM interface actually communicates to a router or a set of routers. The interface from IPATM to the router is an SVC connection. The IPATM interface has configuration that specifies a well-known AESA for the router. When the IPATM interface is configured and attached to VxWorks IP layer, it will perform the following steps.

1. Register the IPATM AESA with the SVC Signalling API (SIGAPI) service.
2. Make a series of SVC call requests to the routers the interface knows about.
3. When a call is established, send an ATMARP request to the router to inform router of the IP address of the IPATM interface.

The SIGAPI provides access to the PXM SAR for the purpose of terminating the SVC on the PXM, and provides a connection establishment procedure for obtaining VC identifiers and procedures for SVC termination.

Note Note that PNNI can be used for routing of call requests from the IPATM interface to IP routers. If PNNI is not available, then static routes must be specified for IPATM to router communication.

Also, router configuration allows the router to route packets from the IPATM interface SVC to a IP host that wishes to manage or access the MGX 8850 Release 2 using TCP/IP clients. This configuration can be separated into two distinct parts:

- The first part involves the configuration needed to interface with the IPATM interface(s) using an SVC.
- The second part involves the configuration required to map data received from a IP host/workstation to the correct SVC for the MGX 8850 Release 2.

The router configuration required for IPATM interface SVC is as follows:

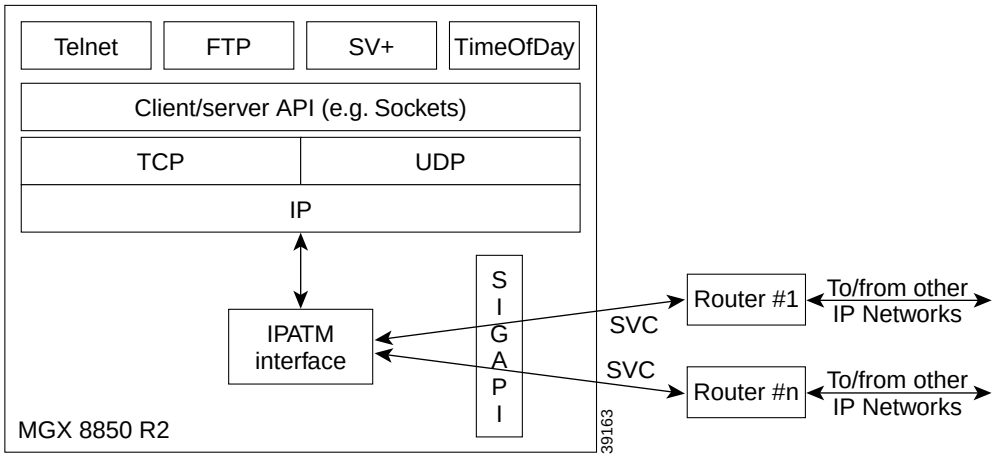
- Creation of IP interface that supports ATM protocol. This interface is assigned an IP address. This address may be on the same subnet as all MGX 8850 Release 2 IPATM interfaces reachable by this router, or may be a unique host route. In the latter case, extra configuration of the router is required to provide IP Host-routing functionality. This is described later in the Limitations and Design section.
- Assignment of well-known ATM End Station Address (AESA) for the router's IP interface. This AESA is to be used by IPATM interfaces to call router.
- If Router's IP interface supports ATMARP (RFC1577) the Router's IP interface is configured to be the ATMARP server for the MGX 8850 Release 2.
- If Router's IP interface does not support ATMARP (RFC1577) assignment of a map table that maps each MGX 8850 Release 2 IP address to the MGX 8850 Release 2 AESA.

The router configuration required for IP host/workstation communication to MGX 8850 Release 2:

- If Router's IP interface supports ATMARP (RFC1577) handle receipt of ATMARP request from MGX 8850 Release 2 IPATM interfaces. Dynamically add the mapping of the IPATM interface's IP address and SVC endpoint to the ATMARP table.
- If Router's IP interface does not support ATMARP (RFC1577) manually configure one IP host-route for each MGX 8850 Release 2 on the router's interface.
- Using a routing protocol (usually RIP), router broadcasts each IP reachable network or list of IP reachable hosts to remote IP host/workstations that are running the same routing protocol. Included in this broadcast will be the subnet or IP addresses of the MGX 8850 Release 2.

Figure A-4 describes the IP router function that provides IP connectivity to MGX 8850 Release 2.

Figure A-4 SVC Interface Between IPATM and Routers



IP Host

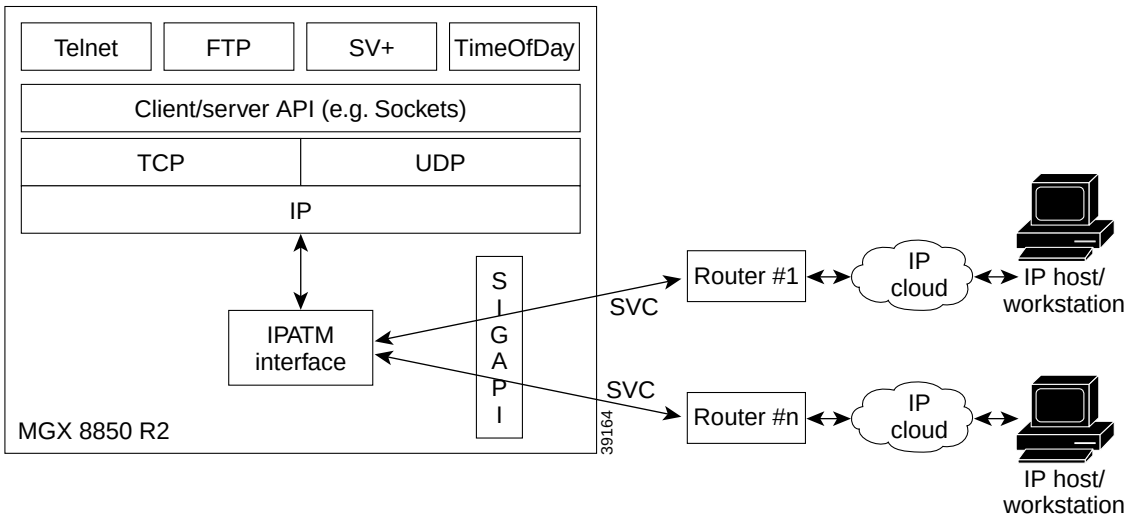
Once the IPATM interface on every MGX 8850 Release 2 is hooked to the IP layer of VxWorks TCP/IP stack and every SVC has been established between IPATM interface and routers, full connectivity will exist between all MGX 8850 Release 2 nodes through all routers. This communication path has also been relayed to the IP host/workstation using a routing protocol such as RIP. The IP host/workstation will now know, via a IP route, which router will accept data for each MGX 8850 Release 2.

Note If the IP host/workstation does not support the routing protocols used by the routers, the IP routes for each MGX 8850 Release 2 will have to be manually added on the CWM workstation.

All that remains for the IP host to do is to determine the IP address for each IPATM interface with which it wants to establish TCP/IP communication. This can be as simple as manually entering these IP addresses into the host's host table, or as complex as dynamically determining these IP addresses via another protocol such as ILMI. In either case it is assumed that the IP host/workstation knows the IP addresses of the IPATM interfaces for the remainder of this chapter.

Figure A-5 shows the complete IP data-path between the MGX 8850 Release 2 and the IP host/workstation. The IP Cloud signifies an IP network and can be as simple as a directly attached ethernet or as complex as a multi-hop, multi-interface type network. Router #1 and Router #2 may or may not be part of the same IP Cloud.

Figure A-5 IP Connectivity Between MGX 8850 Release 2 and IP workstation



Putting It All Together

It is the job of the IP host/workstation to initiate the IP communication to the MGX 8850 Release 2 by sending IP data addressed to the IPATM interface of the MGX 8850 Release 2 to the correct router.

Once received by the router, the IP address of the destination of the data (MGX 8850 Release 2) is looked up in the router's IP route table. Because the IP address of the MGX 8850 Release 2 has been previously added to this interfaces route table, the data is given to the ATM interface driver. There, a map table

specifies which SVC on the router should be used. The ATM interface on the router, if using LLC encapsulation as described in RFC1483, prefixes the data with a header that specifies to the remote end of the SVC that the data is encapsulated IP data. The router then transmits the data onto the SVC.

The encapsulated IP data is received by the MGX 8850 Release 2 IPATM interface on one of its router SVCs. Using RFC1483 if the data is on an SVC supporting LLC encapsulation, IPATM interface strips off the prefixed header and verifies that the data is truly IP data. If it is, the IPATM interface performs a very important function: it adds an entry to a local cache to remember which SVC was used by the IP host/workstation to reach the MGX 8850 Release 2. The cache has the following format:

- IP Address of IP host/workstation
- SVC VC identifier that data was received on
- Timer to be used to time-out the cache entry for the IP host/workstation

Should the cache entry already exist for the IP host/workstation it is updated if the SVC being used has changed. This allows the IPATM interface to dynamically choose the correct SVC necessary. After setting up the cache entry, IPATM interface then adds a new VxWorks IP host-route for the IP host/workstation. The IP host-route will allow VxWorks IP stack to give all IP data that is to be sent to the IP host/workstation to the IPATM interface. Once the IP host-route is set up, the IPATM interface gives the received IP data to VxWorks IP layer. From there, it will be routed to the appropriate server application of the MGX 8850 Release 2.

Should the server application of the MGX 8850 Release 2 need to respond to the data received from the IP host/workstation, it will do so by making a client/server API call to VxWorks. The data from the server will eventually reach the VxWorks IP layer, where a IP route table will be searched to determine the correct interface that should be used for the transmission. The VxWorks IP layer will find the IP host-route that was previously added by the IPATM interface when the data was originally received and the data will be given to IPATM.

The IPATM interface, when given IP data from VxWorks IP layer, will perform a cache lookup of the destination IP address of the data. In the cache, an entry should exist that specifies which SVC VC identifier should be used for sending the IP data. If found, the data is prefixed with a header as described by RFC1483 if the SVC supports LLC encapsulation and sent. If not, the data is dropped and a statistic is kept for the dropped data.

The router will receive the data transmitted by the IPATM interface, strip the RFC1483 header if required, and transmit the data to the correct IP interface for reaching the IP host/workstation. Again, this will be accomplished using a IP route table lookup in the router.

The IP host/workstation will receive the data transmitted by the MGX 8850 Release 2 server and forward the data to the appropriate TCP/IP client running on the host/workstation.

SVC Connections

To configure the type of network as shown in Figure A-1, you must first create an SVC connection between an MGX 8850 Release 2 node (MGX 8850 C) and a router (CWM RTR-1). Configure the connection to MGX 8850 C as your CWM gateway. Next, configure SVC connections between the CWM router and each of the other MGX 8850s.

The following two sections provide information about ample configurations and the features they offer.

Sample Configuration One

The first sample configuration provides the following features:

- Routers support ATMARP and LLC Snap encapsulation
- Routers support ILMI protocol and RIP protocol
- IP Subnet routing used for IP Connectivity network
- PNNI extension not supported for discovering router AESA
- Workstations supports RIP protocol

MGX 8850 Configuration

The following MGX 8850 Release 2 configuration is required:

Step 1 Configure IP address of IPATM interface:

```
ipifconfig atm0 172.24.29.190 arp
```

Step 2 Configure local AESA

```
svcifconfig atm0 local <nsap address > (for example
47.0091.8100.0000.1010.1010.1010.1010.1010.1010.10)
```

Step 3 Configure router AESA of Router

```
svcifconfig atm0 router <nsap address >  (for example
47.0091.8100.0000.0101.0101.0101.0101.0101.0101.01)  arp  llcencap
```

Router Configuration

Step 1 Configure IP address of ATM interface.

```
interface atm 0
ip address atm0 172.29.23.118 255.255.255.0
```

Step 2 Configure local AESA

```
atm nsap-address 47.0091.8100.0000.0101.0101.0101.0101.0101.0101.01
```

Step 3 Configure the router to be ATMARP server:

```
atm arp-server self
```

Step 4 Configure the signalling PVC:

```
atm pvc 1 0 5 qsaal
```

Step 5 Configure UNI 3.1:

```
atm uni-version 3.1
```

Step 6 Ensure that IP routing is enabled:

```
ip routing
```

Sample Configuration 2

The first sample configuration provides the following features:

- Routers do not support ATMARP
- Routers support VC Based Multiplexing encapsulation
- Routers do not support ILMI
- Routers support RIP protocol
- IP Host routing used for IP Connectivity network
- PNNI extension not supported for discovering router AESA
- CWM Workstation does not support RIP protocol

MGX 8850 Configuration

The following MGX 8850 Release 2 configuration is required.

Step 1 Configure IP address of IPATM interface.

```
ipifconfig atm0 172.29.24.190 arp
```

Step 2 Configure local AESA:

```
svcifconfig atm0 local 47.0091.8100.0000.1010.1010.1010.1010.1010.1010.10
```

Step 3 Configure router AESA of Router:

```
svcifconfig atm0 router 47.0091.8100.0000.0101.0101.0101.0101.0101.0101.01 noarp vcmux
```

Router Configuration

You must configure a static route that specifies endpoint for router AESA so that PNNI learns about this endpoint.

Step 1 Configure IP address of ATM interface.

```
interface atm 0
ip address atm0 172.29.23.118 255.255.0.0
```

Step 2 Configure local AESA:

```
atm nsap-address 47.0091.8100.0000.0101.0101.0101.0101.0101.0101.01
```

Step 3 Configure the signalling PVC:

```
atm pvc 1 0 5 qsaal
```

Step 4 Configure UNI 3.1:

```
atm uni-version 3.1
```

Step 5 Manually configure mapping for MGX 8850 Release 2:

```
map-list atm
ip 172.29.24.190 atm-nsap 47.0091.8100.0000.1010.1010.1010.1010.1010.1010.10
```

Step 6 Manually set up IP route table entries for MGX 8850 Release 2:

```
ip route 172.29.24.190 255.255.255.0 172.29.23.118
```

Step 7 Make sure IP routing enabled:

```
ip routing
```

PNNI Link

You must create a PNNI link between the MGX 8850 Release 2 node (for the node which is physically connected to the router) and the router. To create a PNNI link, complete the following described below:

From the AXSM

Step 1 Create a UNI port,

```
popeye10.6.AXSM.a > addport 1 1.1 48000 48000 6 1
```

Step 2 Create a partition,

```
popeye10.6.AXSM.a > addpart 1 1 2 1000000 1000000 1000000 1000000 1 255 33 65535 100 1000
```

From the PXM

Step 1 Display the PNNI ports,

```
popeye10.7.PXM45.a > dsppnports
```

Step 2 Check whether the port is up and normal

```
PortId          IF status         Admin status       ILMI state       Total Activeconns
7.35            up                up                 Undefined        0
7.36            up                up                 Undefined        0
7.37            up                up                 Undefined        0
7.38            up                up                 Undefined        0
6:1.1:1         up                up                 UpAndNormal      1
```

Step 3 If the port is displayed, then do the following:

```
     popeye10.7.PXM45.a > dnpnport 6:1.1:1
     popeye10.7.PXM45.a > cnfpnportsig 6:1.1:1 -univer uni31
     popeye10.7.PXM45.a > uppnport 6:1.1:1

popeye10.7.PXM45.a >
        addaddr  6:1.1:1 47.0091.8100.0000.1010.1010.1010.1010.1010.1010.10  160
```

Note The value of 160 defines the length of the AESA address.

Step 4 If the port is not displayed, then you may need to add the PNNI controller. Please refer to the MGX 8850 Release 2 documentation at the following URL for more information: http://www.cisco.com/univercd/cc/td/doc/product/wanbu/8850r2/index.htm

Note You can issue the **dspsvcif** command to check configuration. Currently, SVCs for in-band management are of UBR CoS.

Networking

The primary goal of your Cisco WAN Manager (CWM) network design is to build the simplest, most economical communication network possible while enabling both flat and tiered networks.

Determination of the number and placement of CWM workstations throughout the network is largely dependent on the amount of message traffic between CWM and the nodes within the network, and the ability of either CWM or the individual MGX™ 8850 series, BPX® 8600 series, or IGX™ 8400 series nodes to process the messages. As each component in the network owns indigenous factors that contribute to overall performance, a key issue becomes understanding the limitation of each component and determining which component is the limiting factor in the network design.

Connecting to Cisco WAN Manager

Each CWM workstation resident within a network must be able to communicate with all nodes within the network.

Each node can have two different IP addresses. The first is the network IP address. You configure the network IP address on a switch by invoking the **cnfnwip** command from the Switch Command Line Interface (CLI). The network IP address is used by CWM to communicate with all nodes in the network.

The second type of IP address, is the LAN IP address. It is configured on a switch by invoking the **cnflan** command from the Switch CLI. CWM uses the LAN IP address for communicating with a gateway node and all feeder nodes.

Note The network and LAN IP addresses should be configured on all of the nodes that are to communicate directly with CWM. All nodes that communicate with the CWM workstation through a gateway node do not need a LAN IP address. These nodes use the network address via the trunks between nodes and are in-band.

Following are descriptions of various components found in a CWM network:

Cisco WAN Manager Gateway Node

A Gateway node provides topology and other vital information about the network to CWM. The Gateway node name is specified in the **/usr/users/svplus/config/network.conf** file on the CWM workstation.

IP Relay

IP Relay is a proprietary protocol used by Cisco WAN switches to pass IP traffic within a Cisco WAN network. The IP Relay function stops at the gateway switch.

IP Relay Gateway

The IP Relay gateway is a node in the WAN network used to relay IP traffic for a group of nodes in the network. When the nodes in the network are geographically distributed, or when the network is large and you created subnets to manage the network, one node in each subnet can be used to relay the IP traffic to all the nodes in that subnet that are connected via trunks. IP Relay traffic will pass through a trunk's Statistical Reserve, but not pass over lines.

Link0 and Link1

CWM and MGX 8230, BPX 8600, or IGX 8400 series nodes use a proprietary protocol to exchange network management information. CWM establishes two types of links (Link0 and Link1) with MGX 8230, BPX 8600, or IGX 8400 series nodes. CWM establishes a Link0 link with the CWM Gateway node, and a Link1 link with all nodes in the network. A Link0 link is also established between CWM and IGX 8400 series feeder nodes.

Four types of network traffic flow between CWM and the Cisco WAN switches that CWM manages, and they are as follows:

- Link0—consists of topology and maintenance messages between the CWM workstation and the CWM gateway node
- Link1—consists of robust messages between the CWM gateway node and other WAN switches
- TFTP—provides file transfers between nodes
- SNMP—provides a communications path to monitor and control network devices, and to manage configurations, statistics collection, performance, and security

CWM only uses SNMP and TFTP to communicate with MGX 8220 nodes.

Ports Used by CWM

This section provides information about ports used by CWM for outgoing and incoming communications.

CWM to Node (Outgoing)

Table B-1 lists the outgoing ports CWM uses to communicate with the nodes.

Table B-1 Outgoing Ports Used by CWM

Protocol	Port	Function
udp	161	SNMP get, set
udp	69	tftp server

Table B-1 Outgoing Ports Used by CWM (continued)

Protocol	Port	Function
tcp	23	telnet
tcp	13	daytime
udp	5120	link 0/1

Node to CWM (Incoming)

Table B-2 lists the incoming ports the nodes use to communicate with CWM.

Table B-2 Incoming Ports Used by CWM

Protocol	Port	Function
udp	162	SNMP Trap
udp	2500	rtm
udp	8161	snmpAgent
tcp	9999	HPOV Database daemon

Configuring Network Management

You have two options for configuring your network for network management. You can use in-band management or out-of-band management.

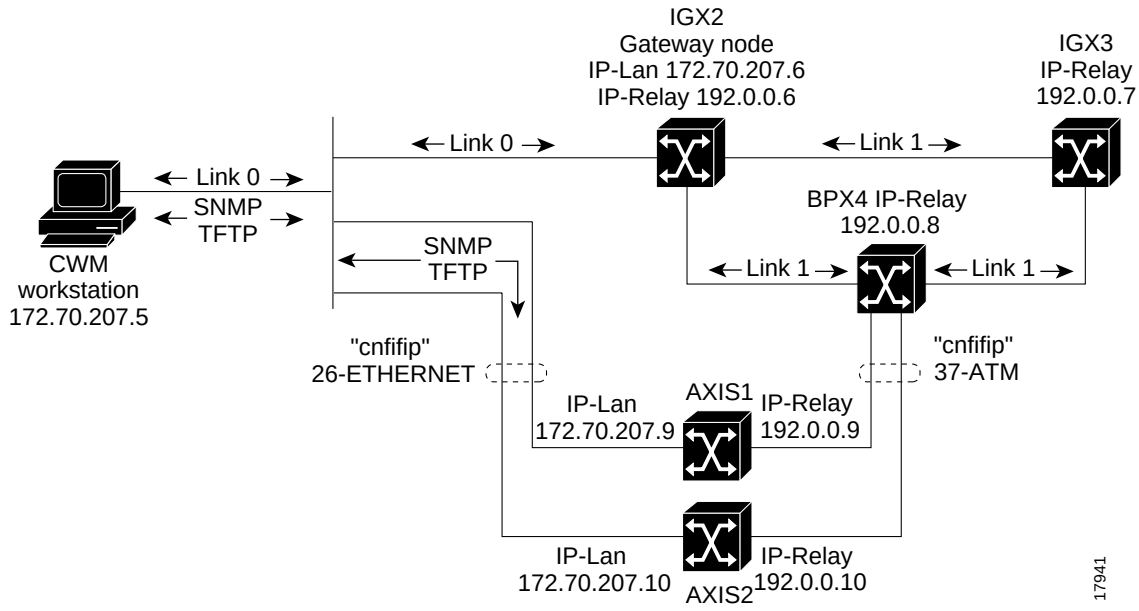
In-Band Management

When using in-band management, the network management traffic flows through the network you are managing. Switch software uses the proprietary IP Relay protocol to pass IP traffic over trunks in the WAN network for in-band management. To use in-band management, at least one node in the network that is to be managed by CWM *must* be connected by way of a LAN, to CWM. This node is called the Gateway node. All network management data from all other nodes in the network flows through the Gateway node to CWM. You can configure CWM to use in-band management using a basic hub attachment without a router or across routers.

In-Band Management Without Routers

Figure B-1 is an illustration of a typical network set up for in-band management without routers. The following configuration of workstation files is required to support in-band management of the network without routers.

Figure B-1 In-Band Management - Basic Hub Attachment Without Router



Note Use valid IP addresses for devices in your network and **avoid using upper-case characters** in the files. The addresses provided in the following examples should be replaced with your network's device addresses.

Step 1 Modify the **/usr/users/svplus/config/network.conf** file to include the name of the Gateway node in the third field to **igx2**, and change the last field (IP Reachability Flag) to **nwip_off**.

The options for the IP Reachability Flag are:

- NWIP_OFF—for in-band management
- NWIP_ON—for out-of-band management

The contents of the **network.conf** file should look similar to the following:

```
NETWORK:Network1
GATEWAYS:igx2
DISCOVERY PROTOCOL:AUTOROUTE
IP REACHABILITY FLAG:NWIP_OFF
```

Step 2 Modify the **/etc/hosts** file to include (along with the file's usual contents) the IP addresses and device names described in Step 3.

Step 3 Modify the **/etc/rc2.d/S72inetsvc** file to add routes by adding a lines similar to the following:

IP Address	Device Name
172.70.207.6	igx2-lan
192.0.0.6	igx2
192.0.0.7	igx3

IP Address	Device Name
192.0.0.8	bpx4
172.70.207.9	mgx1-lan
192.0.0.9	mgx1
172.70.207.10	mgx2-lan
192.0.0.10	mgx2

/usr/sbin/route add net 192.0.0.0 172.70.207.6 1

Add this line after the line similar to the following:

/usr/sbin/route add -*interface* -netmask "240.0.0.0" "224.0.0.0" "$mcastif"

)&

Step 4 Verify your network structures by issuing "**netstat -rn**" and checking the results against the following table.

Table B-3 Results of netstat-rn Command

Routing Table Destination	Gateway	Flags	Ref	Use	Interface
127.0.0.1	127.0.0.1	UH	0	6061	lo0
192.0.0.0	172.70.207.6	UG	0	461	—
172.70.207.0	172.70.207.5	U	3	1311	hme0
224.0.0.0	172.25.70.8	U	3	0	hme0

The following tables provide node configuration information about the nodes shown in Figure B-1, In-Band Management - Basic Hub Attachment Without Router.

Table B-4 Node Configuration (IGX2)

CLI Command	Data
cnfname	igx2
cnflan (IP address, subnet mask, default)	• 172.70.207.6 • 255.255.255.0 • none
cnfnwip (IP address, subnet mask)	• 192.0.0.6 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5
cnfswfunc	Configure/Save/Restore

Table B-4 Node Configuration (IGX2) (continued)

CLI Command	Data
cnffunc	Download/Remote/CWM
cnfsnmp	public, private, public

Table B-5 Node Configuration (MGX)

CLI Command	Data
cnfname	mgx1
cnfifip (26 Ethernet, subnet mask, default)	• 172.70.207.9 • 255.255.255.0 • none
cnfifip (37 ATM, subnet mask)	• 192.0.0.9 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5

Table B-6 Node Configuration (IGX3)

CLI Command	Data
cnfname	igx3
cnflan (IP address, subnet mask, default)	• 0.0.0.0 • 255.255.255.0 • none
cnfnwip (IP address, subnet mask)	• 192.0.0.7 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5
cnfswfunc	Configure/Save/Restore
cnffunc	Download/Remote/CWM
cnfsnmp	public, private, public

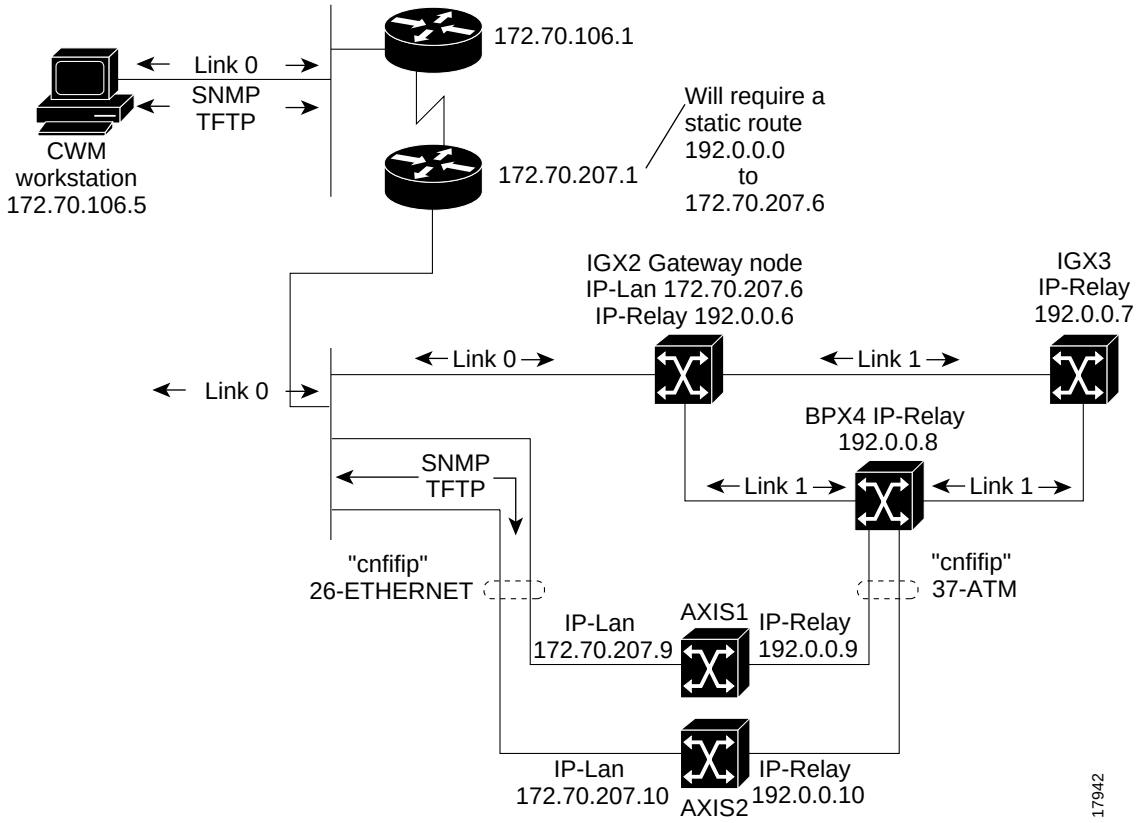
Table B-7 Node Configuration (MGX8220)

CLI Command	Data
cnfname	mgx2
cnfifip (26 Ethernet, subnet mask, default)	• 172.70.207.10 • 255.255.255.0 • none
cnfifip (37 ATM, subnet mask)	• 192.0.0.10 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5

In-Band Management Across Routers

Figure B-2 is an illustration of a typical network set up for in-band management using routers. The following configuration of workstation files is required to support in-band management of the network using routers.

Figure B-2 In-Band Management Using an IP Relay Gateway



Note Use valid IP addresses for devices in your network and **avoid using upper-case characters** in the files. The addresses provided in the following examples should be replaced with your network's device addresses.

Step 1 Modify the **/usr/users/svplus/config/network.conf** file to include the name of the Gateway node in the third field to **igx2**, and change the last field (IP Reachability Flag) to **nwip_off**.

The options for the IP Reachability Flag are:

- NWIP_OFF—for in-band management
- NWIP_ON—for out-of-band management

The contents of the **network.conf** file should look similar to the following:

```
NETWORK:Network1
GATEWAYS:igx2
DISCOVERY PROTOCOL:AUTOROUTE
IP REACHABILITY FLAG:NWIP_OFF
```

Step 2 Modify the **/etc/hosts** file to include the following (along with the usual contents of this file).

IP Address	Device Name
172.70.207.6	igx2-lan
192.0.0.6	igx2
192.0.0.7	igx3
192.0.0.8	bpx4
172.70.207.9	mgx1-lan
192.0.0.9	mgx1
172.70.207.10	mgx2-lan
192.0.0.10	mgx2

Step 3 Modify the **/etc/defaultrouter** file to include the following line:

172.70.106.1 1

Step 4 Modify the **/etc/rc2.d/S72inetsvc** file to add routes by including the following lines:

/usr/sbin/route add default 172.70.108.1 1

/usr/sbin/route add net 192.0.0.0 172.70.106.1 1

Add these lines after the line similar to the following:

/usr/sbin/route add -*interface* -netmask "240.0.0.0" "224.0.0.0" "$mcastif"

Step 5 Verify your network structures by entering **netstat -rn** and checking the results against the following table.

Table B-8 Results of netstat -rn Command

Routing Table Destination	Gateway	Flags	Ref	Use	Interface
127.0.0.1	127.0.0.1	UH	0	6061	lo0
192.0.0.0	172.70.207.6	UG	0	461	
172.70.207.0	172.70.207.5	U	3	1311	hme0
224.0.0.0	172.25.70.8	U	3	0	hme0
Default	172.70.106.1				

The following tables provide node configuration information about the nodes shown in Figure B-2, In-Band Management Using an IP Relay Gateway.

Table B-9 Node Configuration (IGX2)

CLI Command	Data
cnfname	igx2
cnflan (IP address, subnet mask, default)	• 172.70.207.6 • 255.255.255.0 • 172.70.207.1
cnfnwip (IP address, subnet mask)	• 192.0.0.6 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5
cnfswfunc	Configure/Save/Restore

Table B-10 Node Configuration (MGX1)

CLI Command	Data
cnfname	mgx1
ipifconfig (InPci Ethernet, subnet mask, default)	• 172.70.207.9 • 255.255.255.0 • none
ipifconfig (atm0, subnet mask)	• 192.0.0.9 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5

Table B-11 Node Configuration (IGX3)

CLI Command	Data
cnfname	igx3
cnflan (IP address, subnet mask, default)	• 0.0.0.0 • 255.255.255.0 • none
cnfnwip (IP address, subnet mask)	• 192.0.0.7 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5
cnfswfunc	Configure/Save/Restore
cnffunc	Download/Remote/CWM
cnfsnmp	public, private, public

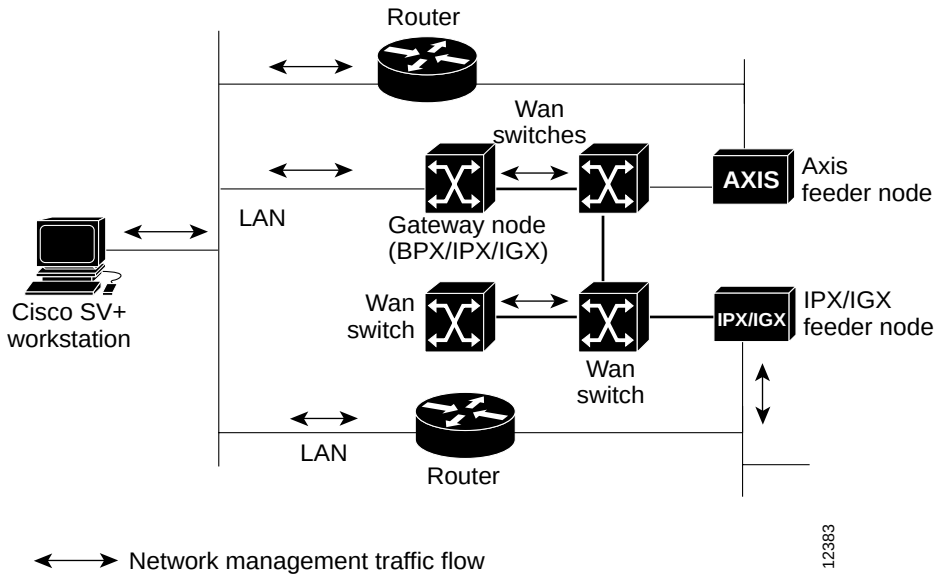
Table B-12 Node Configuration (MGX2)

CLI Command	Data
cnfname	mgx2
ipifconfig (InPCI Ethernet, subnet mask, default)	• 172.70.207.10 • 255.255.255.0 • none
ipifconfig (atm0, subnet mask)	• 192.0.0.10 • 255.255.255.0
cnfstatmast	172.70.207.5
cnffwswinit	170.70.207.5

Out-of-Band Management

With out-of-band management, the traffic flows directly from individual nodes to the Cisco CWM workstation without being routed through the Gateway node. To configure Cisco CWM to use out-of-band management, the last field in the /usr/users/svplus/config/**network.conf** entry should be set to **nwip_on** and direct routes from Cisco CWM to all individual nodes should exist.

Figure B-3 Out-of-Band Management



CWM Out-of-Band Management for MGX8850 (rel2)

Release 10 of CWM always communicates with the Release 2 MGX 8850 nodes using the ATM in-band address. CWM uses the ATM in-band address for topology discovery, trap registration, configuration upload, as well as provisioning. In order to allow CWM to perform out-of-band communication with the switch via the switch's ethernet LAN interface, the static IP route should be configured (on the CWM station and on the router, if necessary) to forward IP traffic destined for an ATM in-band address to the node's ethernet LAN interface. Never configure the same IP address for both ethernet LAN and ATM interfaces.

Configuring an MGX 8850 Feeder Session

This section provides information on how to configure the MGX 8850 switch as a feeder. To set up an MGX 8850 feeder session, complete the following steps:

Step 1 Use the **cnfname** command to assign a name to the MGX 8850 node. The syntax for this command is: **cnfname** <*node name*>

> **cnfname popeye3a**

Step 2 Use the **ipifconfig** command to configure the internet address of the MGX 8850. The syntax for this command is: **ipifconfig** <*interface*> <*IP address*> <*net mask*> <*broadcast address*>

> **ipifconfig InPci 172.29.37.78 255.255.255.000 0**

> **ipifconfig atm0 172.1.1.78 255.255.255.000 0**

> **cnfnwip 172.1.1.78**

Step 3 Use the **dspifip** command to check LAN IP and NWIP

> **dspifip**

```
Interface        Flag  IP Address       Subnetmask       Broadcast Addr
--------------   ----  ---------------  ---------------  ---------------

Ethernet/lnPci0  UP    172.29.37.77     255.255.255.0    172.29.37.255
SLIP/sl0         DOWN  172.29.36.253    255.255.255.252  (N/A)
ATM/atm0         UP    192.9.200.1      255.255.255.128  0.0.0.0
```

Step 4 Use the **addln** command to configure a line. The syntax of this command is **addln** -ds3 <*line number*> | -e3 <*line number*> | -sonet <*line number*>

> **addln -sonet 7.1**

Step 5 Use the **upif** command to add a logical interface to a broadband port on a PXM. The syntax for this command is upif <*if_num*> <*lin_num*> <*pct_bw*> <*min_vpi*> <*max_vpi*>

> **upif 1 1 100 0 4095**

Step 6 Use the **addrscprtn** command to specify the parameters for the resource partitions. The syntax for this command is **addrscprtn** <*if_num*> <*ctrlr_num*> <*ingr_pct_bw*> <*egr_pct_bw*> <*min_vpi*> <*max_vpi*> <*min_vci*> <*max_vpi*> <*max_chans*>

> **addrscprtn 1 1 100 0 4095 0 65535 32767**

Step 7 Use the **cnfswfunc** command to configure the node-level features of the MGX 8850 switch as a feeder node. The syntax of this command is: **cnfswfunc** [<-vsvd enable(yes) | disable<no)>] | [<-ndtype> <fdr | routing>]

> **cnfswfunc -ndtype fdr**

Step 8 Use the **cnfifastrk** command to configure the interface as a feeder trunk. The syntax of this command is: cnfifastrk <*slot.port*><*iftype*>

> **cnfifastrk 7.1 ftrk**

Step 9 Telnet to the BPX® 8600 series switch. (This example assumes that the MGX 8850 trunk is connected to slot 9, line 1.)

> **telnet xxxyyyzzz**

Step 10 Use the **uptrk** command to bring up the trunk.

> **uptrk 9.1**

Step 11 Use the **addshelf** command tobring up the shelf.

> **addshelf 9.1 x**

Step 12 Use the **dsptrks** command to display the trunk status and verify that the trunk is clear.

> **dsptrks**

```
TRK    Current Alarm Status       Other End

7.1     Clear                        bpx4
```

Step 13 At the CWM workstation, enter the following to become the root user.

> **su root <root password>**

#

Step 14 Issue the **route** command to build the route between the 8850 feeder and the BPX.

 # route add net 172.1.1.0 *bpx_IP_address* 1

Step 15 Issue a **ping** command to the MGX 8850 feeder.

ping 172.1.1.78

If the **ping** command is successful, CWM can reach the MGX 8850 feeder node.

User Configurable Network IDs

A new feature in CWM 10.4 gives the user the ability to configure network IDs with a pre-defined network configuration that is specified in the file **network.conf.** In addition to the network name, gateway, and discovery protocol that are specified in this file, the user is able to specify the network ID for each network. The keyword for the network-ID parameter is **NETWORK_ID.**

Note The configurable network ID is only used in Autoroute and PNNI networks. For a standalone network ID, it will always be 32767.

The following is an example of a network configuration in the **network.conf** file:

NETWORK:network2

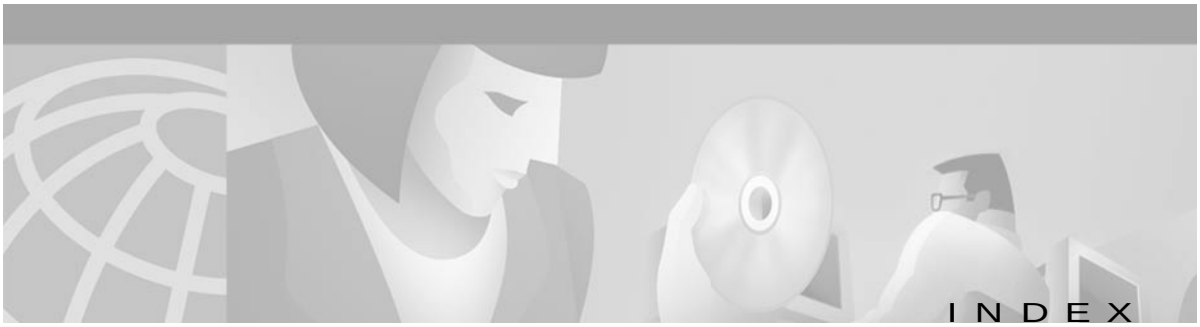
NETWORK_ID:1234

GATEWAYS:popeye2

DISCOVERY PROTOCOL:PNNI

Notes on the network-ID parameter include the following:

- **NETWORK** must be the first parameter in defining the configuration for a network.
- **NETWORK_ID** is optional. If **NETWORK_ID** is not specified in the **network.conf** file, one will be assigned automatically by CWM.
- **NETWORK_ID** must be unique, numeric, and within the range of 1 to 32,000.
- After **NETWORK_ID** is added, modified, or deleted, CWM needs to be cold started.
- To make the CWM gateway work correctly, the *same* **network.conf** file must be used for the Primary and all Secondary CWM workstations.



A

C

D

I

M

N

P

R

S

W