



Cisco WAN Manager Overview

This chapter provides an introduction to Cisco WAN Manager (CWM).

Contents of this chapter include:

- [Introducing CWM](#)
- [CWM Functional Overview](#)

Introducing CWM

CWM is a high-performance element and network management product for service provider networks. Cisco WAN Manager resides at the element and network management layer of the Telecommunications Management Network (TMN) model and integrates with other Cisco applications, such as Cisco Info Center and Cisco Provisioning Center. The high-level applications are Service Level Agreement (SLA) functions, provisioning, fault performance, and accounting management.

CWM manages the Cisco BPX Service Expansion Shelf (SES) and the entire Cisco Advanced ATM Multiservice Portfolio (AAMP). CWM allows network operators to easily monitor usage, quickly provision connections, efficiently detect faults, configure devices, and track network statistics.

CWM also provides robust statistics collection, storing the information in an Informix SQL database and allows simple integration of this data into existing network management and operations systems.

CWM runs on Release 2.8 of Solaris and integrates with Release 6.2 of HP OpenView. For a complete list of CWM software components for Release 12, refer to the *Cisco WAN Manager Installation Guide for Solaris 8, Release 12*.



Note

Release 6.20 of HP OpenView is optional.

Element and network management functions are provided by the CWM system, which can seamlessly manage:

- Cisco MGX 8850 PXM45-based products
- Cisco MGX 8950 PXM45-based products
- Cisco MGX PXM1E-based products (Cisco MGX 8830 and Cisco MGX 8850)
- Cisco MGX PXM1-based products (Cisco MGX 8230, Cisco MGX 8250, and Cisco MGX 8850)
- Cisco SES PNNI Controller
- Cisco IGX 8400 series

- Cisco BPX 8600 series
- Cisco MGX 8220 products

CWM Functional Overview

This section describes the management function of each CWM application as defined in the standard Fault, Configuration, Accounting, Performance, and Security (FCAPS) framework. Many applications have a role in more than one management functional area.

Table 1-1 lists an overview of the CWM applications and management functional area.

Table 1-1 CWM Applications Overview

Name	Fault Management	Configuration Management	Accounting Management	Performance Management	Security Management
Network Topology	X	X	—	—	—
Network Browser	X	—	—	—	—
CiscoView	X	X	—	X	—
Connection Manager	X	X	—	—	—
Config Save/Restore	—	X	—	—	—
SW/FW Images	—	X	—	—	—
Statistics Collection Manager	—	—	X	X	—
Service Class Template Manager	—	X	—	—	—
Security Manager	—	—	—	—	X
CWM Administrator	—	—	—	X	X
Event Browser	X	—	—	X	X
Summary Reports	—	—	—	X	—
Wingz Report Generator	—	—	—	X	—

Table 1-2 describes the FACPS functions.

Table 1-2 Fault, Configuration, Performance, and Security Framework Functions

Name	Description
Fault management	Detects, isolates, corrects, and reports faults for the network and service. Fault management tracks the correlation of related services, for example, reliability, availability, survivability, quality assurance, alarm surveillance, alarm management, fault localization, fault correction, testing, and trouble administration.
Configuration management	Configures and controls network elements, identifies resources, collects information about a resource, and manages connections between network elements. Configuration management deals not only with the state of network elements, but also with the provisioning of resources and services. Generally, configuration management involves network planning, installation, service planning and negotiation, service provisioning, equipment provisioning, status and control, and network topology.
Performance management	Gathers and reports the behavior of network elements, network, and services, which includes quality assurance, monitoring, management control, and analysis.
Accounting management	Collects data that measures network and service usage and enables billing usage. In addition, accounting management controls the flow of funds within the enterprise that includes tariff or pricing, usage measurement, collection and finance, and enterprise control.
Security management	Prevents and detects any improper use of network resources and services as well as recovery from security violations, for example, security, administration, prevention, detection, containment, and recovery.
Planning, modeling, and analysis	Specifies that the planning, modeling, and analysis are treated separately with links to management, for example, fault, configuration, performance, accounting, and security. Planning functions include simulation of networks and management systems, inventory, bandwidth capacity, usage and cost analysis, forecasting, and failure and congestion analysis.

Topology Management

This section describes the network topology management that includes the Network Topology map and Network Browser.

Contents of this section include:

- [Network Topology](#)
- [Network Browser](#)

Network Topology

The Network Topology map represents all the nodes in the network that are discovered by CWM. Each node displays an icon, which uses an industry-standard color scheme that indicates the current alarm status. The map provides Integrated, AutoRoute, Standalone, or private network-network interface

(PNNI) network views; and the center window provides a view of the network as it is automatically presented when the Network Topology main window first appears. Also, the map provides views of the network at different levels, for example, routing nodes or feeder nodes only.

Network element and trunk status are represented by an icon color that changes dynamically. Custom background images are associated with each network map to provide a user-defined view of the network.

The Network Topology's overview window manages a minimized view, which can be displayed in a small window beside the display of the main view. The overview is a periodically generated bitmap of the main view.

The overview also displays a rectangular shaped navigational feature called a Panner that allows resizing, zooming, and panning. Resizing and moving this rectangle with the mouse pointer is reflected in the representation of the overall view. The Network Topology main view zooms in or zooms out by using the Panner, and it is scrolled when the position of the Panner changes.

Release 12 supports the following new features:

- Displays a preferred route and animation.
- CWM manages the PNNI network and is consistent with other CWM stations and the network. If interim local management interface (ILMI) is down, routing trunks between PNNI nodes are not discovered. If a PNNI node is unreachable, the routing trunks connected to it are not discovered.
- Supports multiple peer groups (MPG) for a PNNI logical routing topology.
- Extends support for the Node Resync process to allow for two different levels.
- Supports automatic protection switching (APS) redundancy that is shown in the **Display Trunks** window.

For more information about navigating with the network topology map, see [Chapter 2, "Getting Started with Cisco WAN Manager."](#)

Network Browser

The Network Browser application provides the following functions:

- Represents network information in a hierarchical table format. Each network element managed by CWM has its own attributes and fits in the network's physical or logical hierarchy.
- 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.
- 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 and child relationship.
- Displays informational messages in a multi-line text display. Other types of messages are displayed in response to user actions.
- Launches as a stand-alone application by using the **runNWBrower** command.
- Provides bit error rate test (BERT) diagnostics features.

Release 12 supports the following new features:

- Supports the configuration and operation of the closed user group (CUG).
- Displays the `lmi_type` parameter along with other parameters for the FRSM ports to detect the LMI type. LMI Auto-Sense is configured per port level.

For more information about using Network Browser, see [Chapter 5, "Monitoring Network Faults."](#)

Configuration Management

This section describes the configuration management in CWM that includes both the configuration of individual network elements at the port and line level, and the provisioning of user services, for example, connections.

Contents of this section include:

- [Device Management with CiscoView](#)
- [Connection Manager](#)
- [Service Class Template Manager](#)
- [Software Configuration and Version Management](#)
- [Network Configurator](#)

Device Management with CiscoView

CiscoView communicates with individual network elements, for example, a switch or a concentrator, using Simple Network Management Protocol (SNMP). You can view front and back panel displays that provide a real-time indication of the status of individual cards, lines, and ports.

In addition, you can:

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

For more information about device management using CiscoView, see [Chapter 3, “Managing Devices.”](#)

Connection Manager

Connection Manager allows you to create new connections, display, modify, and delete existing 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, the status for each connection is viewed from one endpoint to the other.

ATM networks support so many connections that it is complicated to administer and manage them. The Connection Service management information base (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, use the 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.

Connection Manager provides fault management capabilities in the form of diagnostic tests for connections, which include continuity (integrity) and round-trip delay time tests for AutoRoute (AR) permanent virtual circuit (PVC) and a route trace facility for PNNI soft permanent virtual connection (SPVC).

CWM provides the capability to provision, monitor, and test hybrid XPVCs for AR and PNNI networks.

Release 12 supports the following new features:

- Supports the following new broadband service types:
 - FRSM12-T3E3 high speed Frame Relay
 - RPM-XF high density routing module
 - AXSM-E
 - AXSM-XG
- Supports AUSM-VISM connections for an XPVC.
- Enables the switch to specify a most desired route for an SPVC that is referred to a preferred route.
- Enables the switch to support PNNI network applications such as data and video broadcast and LAN emulation that is referred to a point-to-multipoint (P2MP) SPVC connection.
- Supports single-ended SPVC connections for ATM, Frame Relay, and RPM connections.

For more information about using the Connection Manager, see [Chapter 4, “Managing Connections.”](#)

Service Class Template Manager

Service Class Template (SCT) Manager allows you to create SCT files that are loaded to nodes, and associated with interfaces on cards within these nodes. You can create custom SCT files in CWM and assign a template ID. Specifically, users or network operators use the SCT application to create, modify, delete, load, and associate SCT files to cards and ports. SCT allows users and network operators to configure FRSM-12, PXM1-E, AXSM, AXSM-B, AXSM-E, and AXSM-XG cards. Each SCT combines two subtemplates that are virtual circuit (VC) parameters and Class of Service Buffer (CoSB) parameters.

In addition, you can:

- Make minor changes to SCT parameters without creating a new SCT ID.
- Rename the SCT file.
- Confirm or resolve version and data discrepancy.

For more information about SCT configuration, see [Chapter 6, “Configuring Service Class Templates.”](#)

Software Configuration and Version Management

Configuration Save and Restore and Software/Firmware Images tools are involved with configuration management.

Node configuration information is stored in battery RAM (BRAM) on Cisco IGX and Cisco BPX switches, or on the hard disk of the node controller for Cisco MGX nodes and the Cisco SES PNNI Controller. You can use the Configuration Save and Restore tool to initiate a backup copy of the node configuration file and store the file on the CWM workstation, or to restore an earlier saved configuration to a specific node. You can backup from multiple nodes of the same type, for example, several Cisco MGX 8230 nodes, using a single configuration save session. The Configuration Save and Restore tool includes a monitor window to monitor the progress of save and restore operations.

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. The Configuration Save and Restore tool significantly reduces time to recover in the unlikely event of a catastrophic failure.

The Software/Firmware Images tool utilizes an Image Download facility to download switch software and firmware images that were previously stored on the CWM workstation.

For more information about software configuration and version management, see [Chapter 9, “Cisco WAN Manager Operations.”](#)

Network Configurator

The Network Configurator is a Java-based, standalone application for CWM that enables users to add new nodes, modify, or delete existing nodes. The Network Configurator provides descriptor information, node name, and IP address information for the nodes in your network.

For more information about launching and using the Network Configurator, see the [Chapter 2, “Getting Started with Cisco WAN Manager.”](#)

Performance Management

The performance management function in CWM involves the system’s ability to collect and store massive amounts of statistical data for network activity.

Contents of this section include:

- [Statistics Collection Manager](#)
- [Summary Reports and Wingz Reports](#)

Statistics Collection Manager

The Statistics Collection Manager (SCM) is a distributed process that collects statistics from network nodes at defined intervals, and accumulates the statistics in the statistics database. SCM is also a standalone collector that allows a separate SCM collection server in both installation and statistics collection. You 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.

By using the SCM, you define the network objects, which are connections, ports, trunks, and the types of statistics that are collected from each object on single or multiple nodes. You also define the bucket interval, which is the statistics sampling rate and granularity of the collected data. 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.

You can also use the Standalone Stats Manager (SSM) and ScmProxy to configure the statistics collection.

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 through the SQL architecture because of the large volume of information present in the database and the inefficiencies involved in retrieving it through SNMP.

The following list contains examples of port and virtual channel level statistics that are used to support operations and maintenance, customer network management, and usage-based billing:

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

Release 12 supports the following new features:

- Displays the SCM Gateway Monitor that is separated from the CWM Gateway Monitor.
- Configures the SSM that resides in a separate workstation and not in the CWM workstation. CWM and SSM communicate through WANDEST.
- Adds and deletes the Standalone Stats Collector (SSC) in the SCT Manager.
- Provides an updated ScmProxy host file.
- Provides new statistics types for AUSM, FRSM, and PXM1 cards.
- Collects new PNNI statistics.

For more information about using the Statistics Collection Manager, see [Chapter 7, “Collecting Statistics.”](#)

Summary Reports and Wingz Reports

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. The 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.

You cannot launch Summary Reports and Wingz Reports from the **Apps** pull-down menu. For information about launching Summary Reports and Wingz Reports, see [Chapter 8, “Generating Reports.”](#)



Note

Wingz Report is an optional module.

Fault Management

This section describes the applications and functions for fault management.

Contents of this section include:

- [Event Browser](#)
- [Peer-to-Peer Communications](#)
- [Gateway Monitor](#)

Event Browser

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 are 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 are configured on a per-node basis such that the same type of event from different sources cause different automatic actions.

For more information about using the Event Browser, see [Chapter 5, “Monitoring Network Faults.”](#)

Peer-to-Peer Communications

CWM allows multiple CWM workstations to manage a network with improved network synchronization and scalability, and better handling of peer-to-peer communications failure scenarios. An automatic switchover feature (AutoSwitchOver) is designed to help a Secondary CWM get out of the degraded mode of operation, without requiring a restart of the CWM core on either the Primary CWM or Secondary CWM. In most cases, a Secondary CWM gets out of the degraded mode of operation automatically within a limited period of time.

In addition to the AutoSwitchOver feature, peer-to-peer communications include a bidirectional heartbeat feature, which allows for better efficiency in the sending and checking of heartbeat messages, and also makes it possible for a Primary CWM to detect and report the connectivity status of Secondary CWMs. Also, a more reliable mechanism for reporting communication problems through SNMP traps generation for critical CWM-CWM events can expedite users reaction to the problems that can affect peer-to-peer communications.

When communications between a Primary CWM and Secondary CWM are interrupted, users are able to continue the provisioning of network data. If for any reason the communication between CWM servers are interrupted, provisioning for user data is suspended on the Secondary CWM. However, provisioning for user data continues on the Primary CWM. During that time, the provisioning of user data and monitoring of the network are not impacted.

Release 12 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.

For more information about peer-to-peer communications, see [Appendix A, “Cisco WAN Manager Peer-to-Peer Communication.”](#)

Gateway Monitor

The Gateway Monitor feature provides you with CWM gateway information that includes the CWM workstation's role as the Primary CWM, Secondary CWM, or Tertiary CWM. The gateway feature also communicates whether or not the CWM workstation's connection to the Primary CWM is up or down (if it is not the Primary CWM), and what the current synchronization status is for the CWM workstation.

For more information about the CWM Gateway Monitor, see [Appendix A, "Cisco WAN Manager Peer-to-Peer Communication."](#)

Accounting Management

CWM does not include any dedicated application for accounting or billing. However, the CWM statistics collection process generates the basic usage data that is required by an accounting system to generate customer-billing records.

The statistics in the CWM database are retrieved by using industry-standard SQL tools, and exported to an external accounting system based on an application provided by a third-party or a proprietary billing system developed by the Service Provider.

Security Management

This section describes the applications that are used for security management.

Contents of this section include:

- [Security Manager](#)
- [CWM Administration](#)

Security Manager

With the CWM Security Manager application, you can create access profiles for different categories that limit users in that category to certain CWM applications, and to specific actions using those applications.

When assigning a new user account on CWM, you need to assign that user a UNIX login and password, and then create a user profile with Security Manager. The user access profiles are based on the following functions:

- Read
- Create
- Modify
- Delete

Security Manager also 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.

Release 12 supports the following new features:

- Provides audit trail support to monitor and track for user activities. The log includes user, action, time, and date.
- Accesses community strings and FTP passwords by using the **nodeinfocfg** command.

For more information about using security manager, see [Chapter 2, “Getting Started with Cisco WAN Manager.”](#)

CWM Administration

The CWM Administration application monitors users, audits logs, and processes on the CWM Server.

Release 12 supports the following new features:

- Shows user information (username, client hostname, and application name) of all users logged in to the CWM client applications.
- Views audit logs.
- Views CWM Server process state.

The user and process tabs are automatically updated when there are any changes. The audit logs are retrieved whenever you changed and submitted the filter criteria and clicked **Submit**.

For more information about using CWM Administration, see [Chapter 2, “Getting Started with Cisco WAN Manager.”](#)

