CiscoWorks Blue Maps and SNA View Workstation Installation and Administration Guide

Release 3.0.1

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-7811351=
Text Part Number: 78-11350-02

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The following information is for FCC compliance of Class A devices: This equipment has been tested and found to comply with the limits for a Class A digital device, pursuant to part 15 of the FCC rules. These limits are designed to provide reasonable protection against harmful interference when the equipment is operated in a commercial environment. This equipment generates, uses, and can radiate radio-frequency energy and, if not installed and used in accordance with the instruction manual, may cause harmful interference to radio communications. Operation of this equipment in a residential area is likely to cause harmful interference, in which case users will be required to correct the interference at their own expense.

The following information is for FCC compliance of Class B devices: The equipment described in this manual generates and may radiate radio-frequency energy. If it is not installed in accordance with Cisco's installation instructions, it may cause interference with radio and television reception. This equipment has been tested and found to comply with the limits for a Class B digital device in accordance with the specifications in part 15 of the FCC rules. These specifications are designed to provide reasonable protection against such interference in a residential installation. However, there is no guarantee that interference will not occur in a particular installation.

Modifying the equipment without Cisco's written authorization may result in the equipment no longer complying with FCC requirements for Class A or Class B digital devices. In that event, your right to use the equipment may be limited by FCC regulations, and you may be required to correct any interference to radio or television communications at your own expense.

You can determine whether your equipment is causing interference by turning it off. If the interference stops, it was probably caused by the Cisco equipment or one of its peripheral devices. If the equipment causes interference to radio or television reception, try to correct the interference by using one or more of the following measures:

• Turn the television or radio antenna until the interference stops.

• Move the equipment to one side or the other of the television or radio.

• Move the equipment farther away from the television or radio.

• Plug the equipment into an outlet that is on a different circuit from the television or radio. (That is, make certain the equipment and the television or radio are on circuits controlled by different circuit breakers or fuses.)

Modifications to this product not authorized by Cisco Systems, Inc. could void the FCC approval and negate your authority to operate the product.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

CHAPTER 11

About This Guide

This chapter describes the objectives, audience, organization, and conventions of the *CiscoWorks Blue Maps and SNAView Workstation Installation and Administration Guide*. It also points to related publications and sources of information.

Document Objectives

This guide tells you how to perform the following tasks:

- Prepare to install CiscoWorks Blue Maps and SNA View.
- Install, configure, and start CiscoWorks Blue Maps and SNA View.
- Discover devices and perform other administration tasks using the CiscoWorks Blue Administration interface.
- Control and monitor the CiscoWorks Blue processes using the CiscoWorks Blue Process Manager interface.
- Verify that end users can view the Maps and SNA View information.
- Control and view the messages logged by CiscoWorks Blue processes using the CiscoWorks Blue Message Logger interface.
- Diagnose problems with CiscoWorks Blue Maps and SNA View.
- Understand CiscoWorks Blue Maps and SNA View database table structures.

For last-minute information about using the CiscoWorks Blue Maps and SNA View applications, see the *Release Notes for CiscoWorks Blue Maps and SNA View Software Release 3.0*.

Audience

This guide is for the network administrator or operator who installs and configures CiscoWorks Blue Maps or SNA View software.

Users of UNIX workstations should be familiar with the following topics:

- Motif window management system and/or web browsers
- A network management system such as TME10 NetView for AIX, HP OpenView, or SunNet Manager
- Basic UNIX commands
- UNIX text editors

Document Organization

This guide contains information pertaining to using CiscoWorks Blue on UNIX workstations. CiscoWorks Blue Maps and SNA View 3.0 are both supported on AIX, HP, and Solaris UNIX platforms.

This guide is divided into the following chapters and appendices:

- Chapter 1, "CiscoWorks Blue Maps and SNA View Features," introduces the functions provided by the CiscoWorks Blue Maps and SNA View applications.
- Chapter 2, "Preparing to Install CiscoWorks Blue Applications," describes software and hardware prerequisites and methods of verifying compliance on various workstation platforms. It also tells you how to become the root user so that you will be authorized to install the product.
- Chapter 3, "Installing and Configuring CiscoWorks Blue," provides procedures for installing and configuring the applications on an IBM AIX, HP UNIX (HP-UX), or Sun Solaris platform.

- Chapter 4, “Monitoring and Controlling CiscoWorks Blue Applications,” describes how to use the CiscoWorks Blue applications to administer the product.
- Chapter 5, “Using the Process Manager,” describes how to start and use the Process Manager to start and control the processes.
- Chapter 6, “Using the Message Log Viewer,” describes how to use the message log viewer to review the messages collected from the applications.
- Chapter 7, “Using the Administration Application,” describes how to start and use the CiscoWorks Blue Administration program to add, delete, and modify devices, discover the network, and specify DLSw key devices.
- Chapter 8, “Starting the User Applications,” describes how to start the DLSw, RSRB, and Advanced Peer-to-Peer Networking (APPN) Motif applications and the web server from a workstation.
- Chapter 9, “Improving Performance,” describes ways to improve the performance of the workstation applications.
- Chapter 10, “Event Notification Messages,” describes the TRAP messages that the DLSw and APPN applications can send to the workstation network management system (NMS) when changes in network status occur.
- Chapter 11, “Troubleshooting CiscoWorks Blue Applications,” tells you how to recognize symptoms and solve the related problems with the workstation application.
- Appendix A, “Controlling PU and LU Activation and Deactivation,” tells you how to enable and disable the activation and deactivation of LUs and PUs.
- Appendix B, “Mounting a CD-ROM on UNIX Workstations,” describes procedures for exporting and mounting CD-ROMs on local and remote workstations.
- Appendix C, “Database Tables,” describes the structure of the Maps and SNA View database tables.
- Appendix D, “CiscoWorks Blue Commands and Processes,” tells you how to start and stop processes, and it describes the relationship between the processes and the database tables.

- Appendix E, “CiscoWorks Blue Maps and SNA View Web Interface,” provides information about accessing various functions of the CiscoWorks Blue Maps and SNA View applications by supplying a URL containing function calls and parameters.
- Appendix F, “Mainframe and Workstation Installation Checklist,” is a checklist that you can use to communicate important installation information between the Maps or SNA View workstation installer and the mainframe installer.

Document Conventions

This guide uses basic conventions to represent text and table information.

Product names use these conventions:

- Cisco Works Blue refers to both Maps and SNA View applications.
- Maps refers to the Motif applications and protocol-oriented web applications.
- SNA View refers to the LU/PU portion of the web application.

Command descriptions use these conventions:

- Commands and keywords are in **boldface** font.
- Arguments for which you supply values are in *italic* font.
- Elements in square brackets [ ] are optional.
- Alternative but required keywords are grouped inside braces { }. Alternative selections are separated by a vertical bar (|).

Examples use these conventions:

- Terminal sessions and information the system displays are printed in a `screen` font, with default responses in square brackets ([ ]).
- Information you enter is in **boldface** font. Variables you enter are printed in *italic* font.
- Nonprinting characters, such as passwords, are shown in angle brackets (< >).

This publication also uses the following conventions:

- Menu items and button names are in **boldface** font.
- A menu item you are to select is indicated by the following convention: Select **Admin > Discover > Seed File**.
- Directories and filenames are in *italic* font.

Timesaver Means *the described action saves time*. You can save time by performing the action described in the paragraph.

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

Caution Means *reader be careful*. You are capable of doing something that might result in equipment damage or loss of data.

Related Documentation

The CiscoWorks Blue Maps and SNA View documentation set includes the following documentation:

- *Release Notes for CiscoWorks Blue Maps and SNA View Software Release 3.0.1*
- *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide*
- *CiscoWorks Blue Maps and SNA View Workstation Installation and Administration Guide*

- *CiscoWorks Blue Maps and SNA View User Guide*
- CiscoWorks Blue Maps Online Help System
- Installation Checklist for CiscoWorks Blue Maps and SNA View for UNIX
- Quick Start for CiscoWorks Blue SNA View for UNIX

Online Help

CiscoWorks Blue Maps and SNA View include an online help system that allows users to access different levels of help information. The system provides overviews, related information, procedures, and glossary data for the applications and features. It contains both keyword and full-text search capabilities to enable users to search for specific text within the online help system.

Obtaining Documentation

Cisco provides several ways to obtain documentation, technical assistance, and other technical resources. These sections explain how to obtain technical information from Cisco Systems.

Cisco.com

You can access the most current Cisco documentation on the World Wide Web at this URL:

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

You can access the Cisco website at this URL:

http://www.cisco.com

International Cisco websites can be accessed from this URL:

http://www.cisco.com/public/countries_languages.shtml

Documentation CD-ROM

Cisco documentation and additional literature are available in a Cisco Documentation CD-ROM package, which may have shipped with your product. The Documentation CD-ROM is updated regularly and may be more current than printed documentation. The CD-ROM package is available as a single unit or through an annual or quarterly subscription.

Registered Cisco.com users can order a single Documentation CD-ROM (product number DOC-CONDOCCD=) through the Cisco Ordering tool:

http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html

All users can order monthly or quarterly subscriptions through the online Subscription Store:

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

Ordering Documentation

You can find instructions for ordering documentation at this URL:

http://www.cisco.com/univercd/cc/td/doc/es_inpck/pdi.htm

You can order Cisco documentation in these ways:

- Registered Cisco.com users (Cisco direct customers) can order Cisco product documentation from the Networking Products MarketPlace:

  http://www.cisco.com/en/US/partner/ordering/index.shtml

- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco Systems Corporate Headquarters (California, U.S.A.) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

You can submit comments electronically on Cisco.com. On the Cisco Documentation home page, click **Feedback** at the top of the page.

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

You can submit comments by using the response card (if present) behind the front cover of your document or by writing to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com offers a suite of interactive, networked services that let you access Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com provides a broad range of features and services to help you with these tasks:

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

To obtain customized information and service, you can self-register on Cisco.com at this URL:

http://tools.cisco.com/RPF/register/register.do

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available: the Cisco TAC website and the Cisco TAC Escalation Center. The type of support that you choose depends on the priority of the problem and the conditions stated in service contracts, when applicable.

We categorize Cisco TAC inquiries according to urgency:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration. There is little or no impact to your business operations.
- Priority level 3 (P3)—Operational performance of the network is impaired, but most business operations remain functional. You and Cisco are willing to commit resources during normal business hours to restore service to satisfactory levels.
- Priority level 2 (P2)—Operation of an existing network is severely degraded, or significant aspects of your business operations are negatively impacted by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.
- Priority level 1 (P1)—An existing network is “down,” or there is a critical impact to your business operations. You and Cisco will commit all necessary resources around the clock to resolve the situation.

Cisco TAC Website

The Cisco TAC website provides online documents and tools to help troubleshoot and resolve technical issues with Cisco products and technologies. To access the Cisco TAC website, go to this URL:

http://www.cisco.com/tac

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

http://tools.cisco.com/RPF/register/register.do

If you are a Cisco.com registered user, and you cannot resolve your technical issues by using the Cisco TAC website, you can open a case online at this URL:

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

If you have Internet access, we recommend that you open P3 and P4 cases online so that you can fully describe the situation and attach any necessary files.

Cisco TAC Escalation Center

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

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

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

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

Obtaining Additional Publications and Information

Information about Cisco products, technologies, and network solutions is available from various online and printed sources.

- The *Cisco Product Catalog* describes the networking products offered by Cisco Systems, as well as ordering and customer support services. Access the *Cisco Product Catalog* at this URL:

  http://www.cisco.com/en/US/products/products_catalog_links_launch.html

- Cisco Press publishes a wide range of networking publications. Cisco suggests these titles for new and experienced users: *Internetworking Terms and Acronyms Dictionary, Internetworking Technology Handbook, Internetworking Troubleshooting Guide*, and the *Internetworking Design Guide*. For current Cisco Press titles and other information, go to Cisco Press online at this URL:

http://www.ciscopress.com

- *Packet* magazine is the Cisco quarterly publication that provides the latest networking trends, technology breakthroughs, and Cisco products and solutions to help industry professionals get the most from their networking investment. Included are networking deployment and troubleshooting tips, configuration examples, customer case studies, tutorials and training, certification information, and links to numerous in-depth online resources. You can access *Packet* magazine at this URL:

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

- iQ Magazine is the Cisco bimonthly publication that delivers the latest information about Internet business strategies for executives. You can access iQ Magazine at this URL:

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

- Internet Protocol Journal is a quarterly journal published by Cisco Systems for engineering professionals involved in designing, developing, and operating public and private internets and intranets. You can access the Internet Protocol Journal at this URL:

  http://www.cisco.com/en/US/about/ac123/ac147/about_cisco_the_internet_protocol_journal.html

- Training—Cisco offers world-class networking training. Current offerings in network training are listed at this URL:

  http://www.cisco.com/en/US/learning/le31/learning_recommended_training_list.html

- You can access the CiscoWorks Blue web page using the following URL:

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

CHAPTER 1

CiscoWorks Blue Maps and SNA View Features

This chapter introduces the functions and capabilities of CiscoWorks Blue Maps and SNA View. CiscoWorks Blue Maps and CiscoWorks Blue SNA View provide a set of Motif and Web-based applications for diagnosing problems in, and managing, integrated networks based on Systems Network Architecture (SNA) and Transmission Control Protocol/Internet Protocol (TCP/IP) environments.

This chapter includes the following main sections:

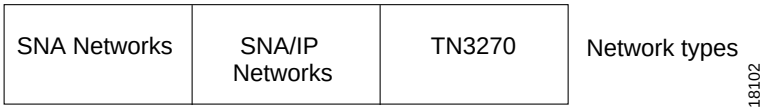
SNA Network Configurations

The world of SNA networking is divided into the following three fundamental environments:

- Traditional SNA networks, in which the mainframe computer, the network, and the network nodes are all running native SNA networking protocols.
- Integrated SNA/IP networks, in which the mainframe computer and the network nodes are running SNA protocols, which are being communicated over a TCP/IP network usually containing routers running remote source-route bridging (RSRB), data-link switching (DLSw), or Advanced Peer-to-Peer Networking with SNA Switching Services (APPN/SNASw) over IP.
- TN3270 networks, in which the mainframe computer is running SNA protocols while the network nodes and the network itself are running TCP/IP.

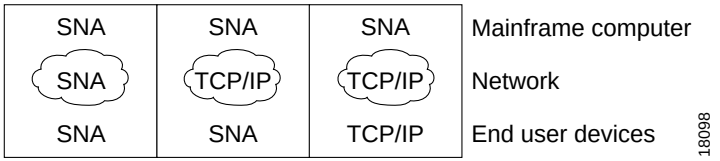
Figure 1-1 shows the types of SNA networks.

Figure 1-1 SNA Network Types



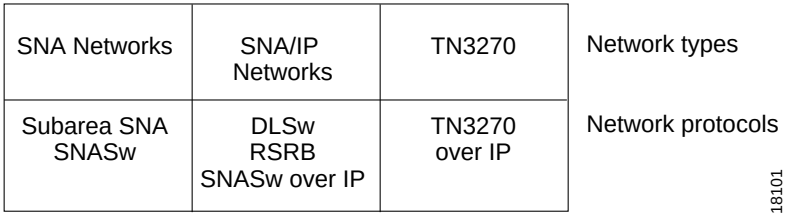
In these SNA networks, the mix of protocols run by the mainframe computer, the network, and the end-user devices varies, as shown in Figure 1-2.

Figure 1-2 Various SNA Network Protocols



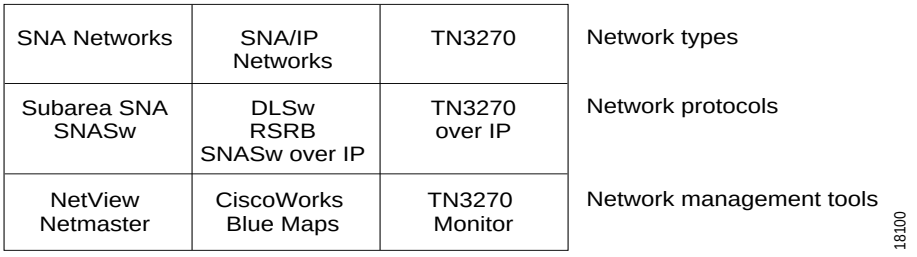
These various SNA networks run a variety of protocols to transport data between the mainframe computer and the network nodes over the network. The SNA network protocols are shown in Figure 1-3.

Figure 1-3 SNA Protocols



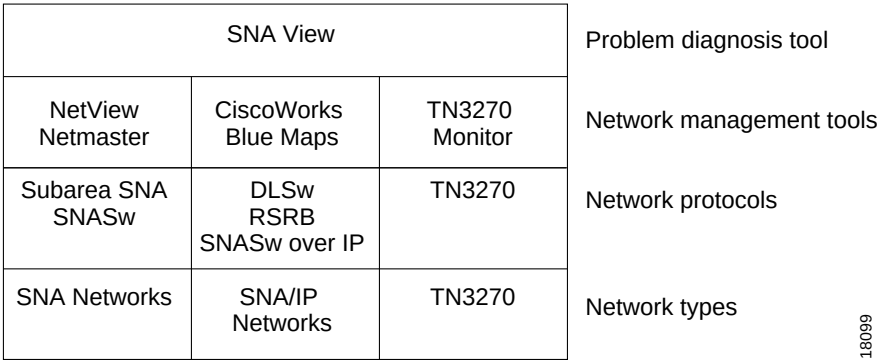
Network management programs, which are tools that you use to manage these SNA networks, also vary depending on the protocols used, as shown in Figure 1-4.

Figure 1-4 SNA Network Management Tools



There is one tool that lets you identify and isolate outages in all SNA networks. SNA View, as shown in Figure 1-5, lets you see network connectivity views for the three types of SNA networks.

Figure 1-5 SNA Problem Diagnosis Tool



Network Management and Problem Diagnosis

When managing SNA networks, diagnosing problems, the distinctions between diagnosis and management must be clear:

- When you diagnose an SNA network problem, you are reacting to a specific, often reported, network problem. The usual scenario develops when a network outage occurs and a network user is stranded without a connection, and your help line or technical response telephone begins to ring. The end result of problem diagnosis is to detect where the problem is and diagnose the cause.
- When you manage an SNA network, you are looking at a broader view of the network, and you might be trying to manipulate the status of one or more network devices to repair an outage or to improve performance. You might be called as a result of problem diagnosis, when a help-line responder detects an inactive device and asks you to activate it. But your job might also require you to take broader views of network maps to see where bottlenecks occur and to reroute network traffic.

Cisco offers a set of SNA network management and problem diagnosis tools to help you perform these tasks.

- CiscoWorks Blue SNA View is a tool for problem solving in all SNA networks. Its purpose is to collect as much information about the outage as possible, and then to show you a picture of all the network devices between the inactive network node and the mainframe computer.
- CiscoWorks Blue Maps is a tool for network management for those networks in which SNA is routed over IP networks using DLSw, RSRB, or APPN/SNASw. Its purpose is to give you an overview of your integrated SNA/IP networks and to let you manage the IP routers that make up the network.
- When you use the CiscoWorks Blue SNA View application, you can start with a few bits of information about a network outage, perhaps the logical unit (LU) name or the MAC address, and view the entire path from a network terminal back through the network of routers or communication controllers to the SNA mainframe computer. When you use the CiscoWorks Blue Maps applications, you can manage the Cisco routers that control communication in networks that are enabled for RSRB, DLSw, or APPN/SNASw.

SNA Resource Management

There is a trend in network management to reduce the need for separate network resource managers by providing direct management of heterogeneous multi-vendor networks from a single, integrated network management system (NMS). In keeping with this strategy, CiscoWorks Blue uses information from Virtual Telecommunications Access Method (VTAM) and the Multiple Virtual Storage system (MVS) to enable network administrators to monitor and manage SNA resources. To further simplify and enhance network management, use CiscoWorks Blue Maps to display your SNA resources on graphical network maps.

The CiscoWorks Blue workstation program collects SNA network information provided by the Maps and SNA View mainframe program. It provides the SNA control and correlation needed to manage SNA devices from a UNIX workstation, allowing the network administrator to see beyond the routers to the SNA physical unit (PU) and LU resources.

CiscoWorks Blue gets PU and LU resource information from VTAM at a mainframe computer and correlates that information with the Cisco routers that are associated with the PUs and LUs. By interacting with the mainframe, CiscoWorks Blue adds vital PU and LU information to the graphical maps.

Because CiscoWorks Blue correlates PU and LU names with the routers in the network, you can more easily isolate problems to the IP network or to the SNA network.

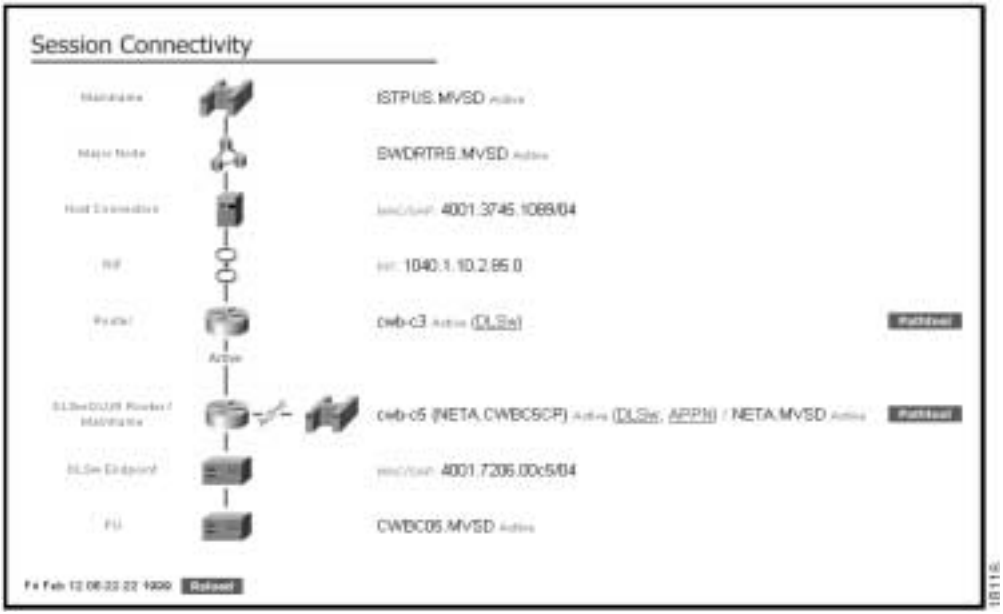
Resource information is dynamically updated to provide a snapshot of the network as it appears at any given time. This information allows the administrator to display a graphical map that depicts details from the PU back toward the VTAM host, providing information, such as the PU and LU status and the PU and LU dependency relationships.

Note PUs connecting to the mainframe using the RSRB protocol and a CIP router or a 3172 Interconnect Controller do not benefit from the correlation feature. This means that Maps applications cannot determine the routers on which these PUs are dependent for connectivity to the mainframe. However, the IBM APAR OW36070 is available that allows Maps and SNA View to support switched PUs using these types of connections.

Introducing CiscoWorks Blue SNA View

This section presents a brief overview of the functions provided by CiscoWorks Blue SNA View. SNA View is a web-based application. The SNA View web server gathers information about routers and SNA LUs and PUs from the SNA View and Maps database. When you link to the SNA View web page, you can display SNA session paths. The web page then displays a session connectivity view, as shown in Figure 1-6.

Figure 1-6 SNA View Session Connectivity View



What SNA View Provides

The CiscoWorks Blue SNA View product is a tool for problem diagnosis in all SNA networks.

CiscoWorks Blue SNA View offers web-based client and server applications. These applications start with as much information about a failing node as you can provide and then display the network devices between that node and the mainframe computer.

Introducing CiscoWorks Blue Maps

CiscoWorks Blue Maps is a set of applications that let you manage Cisco routers in an IBM SNA network. Each Maps application focuses on a particular protocol: DLSw, RSRB, or APPN/SNASw. Maps displays graphical views of SNA networks connected with Cisco routers. These views are dynamically updated to provide snapshots of the network as it appears at any time.

Maps also lets you see beyond the routers to the SNA PUs and LUs that use the DLSw, RSRB, or APPN/SNASw protocols. The Maps mainframe component discovers the PUs and LUs from VTAM information at the mainframe, monitors those PUs and LUs, and reports their changing status to the Maps workstation applications to update the Maps database and the graphical maps.

What Maps Provides

The CiscoWorks Blue Maps product provides the following Motif and web-based applications that show, in a graphical or tabular format, the routers that make up your integrated SNA and TCP/IP network:

- DLSw Motif-based application—Displays graphic maps of DLSw devices and includes dependency views back to an SNA mainframe computer from SNA LUs and PUs that use DLSw.
- RSRB Motif-based application—Displays graphic maps of RSRB devices and includes dependency views back to an SNA mainframe computer from SNA LUs and PUs that use RSRB.

- APPN/SNASw Motif-based application—Displays graphic maps of APPN/SNASw devices and includes dependency views back to an SNA mainframe computer from SNA LUs and PUs that use APPN/SNASw over IP.
- HTML interface to Maps—Provides DLSw, RSRB, and APPN/SNASw network information in tabular format, but does not include dependency views from SNA LUs and PUs (SNA View provides these views).

Maps Features

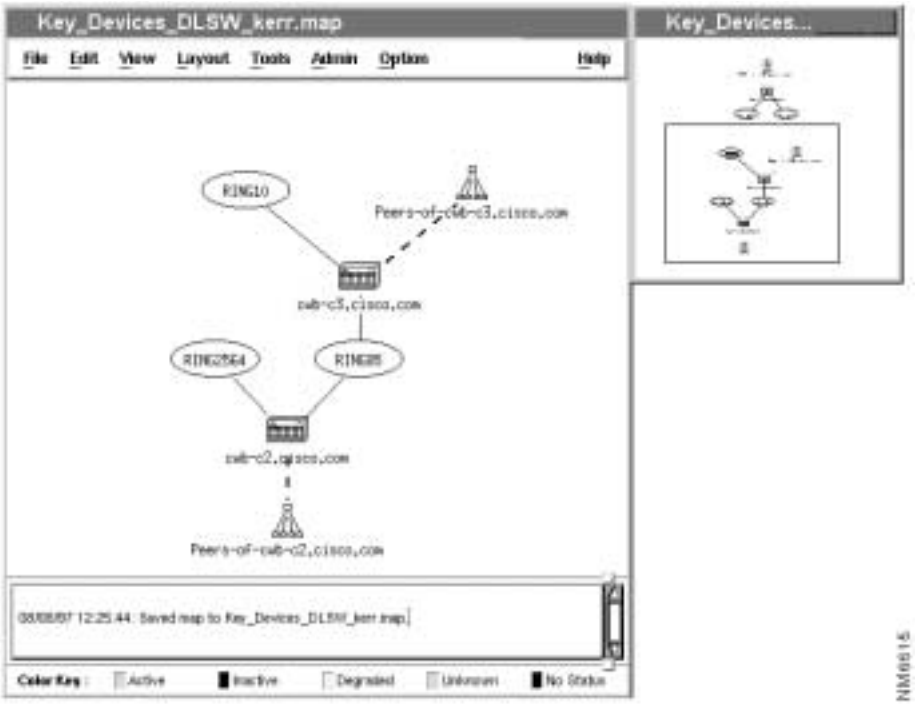
CiscoWorks Blue Maps applications provide the following features:

- Graphical Map Layout, page 1-9
- Network Management Tools, page 1-10
- Problem Determination, page 1-11

Graphical Map Layout

CiscoWorks Blue Maps applications get network data from the MIBs to provide detailed logical maps of the SNA-related protocols. These maps are automatically drawn to depict specific protocols in the network. For example, the DLSw key devices map provides a view of the key DLSw routers with their peer routers and the rings and peer connections between them. Topology is drawn based on the DLSw protocol, and you can focus on different components of the DLSw network such as individual routers and links. Figure 1-7 is a sample DLSw key devices view. It shows you a small set of routers that you designate as “key devices” based on their networking attributes. This map also shows you the peer routers to those key routers, and it shows you the peer connections that connect the key routers to their peers.

Figure 1-7 Sample DLSw Map



Network Management Tools

CiscoWorks Blue Maps provides the network administrator with the tools needed to manage growing integrated SNA and TCP/IP networks. This set of Maps applications (RSRB, DLSw, and APPN/SNASw) can be integrated with popular Simple Network Management Protocol (SNMP) management platforms such as IBM NetView for AIX, HP OpenView, or SunNet Manager. From the graphical maps, you can display path information or go directly to a device view using CiscoView.

Problem Determination

You can use the graphical maps to efficiently identify and diagnose problems related to the specific protocol under observation (RSRB, DLSw, and APPN/SNASw). Having identified the problem area, you can easily access additional information by invoking other menus in the application. For instance, in a DLSw network, you can use a key routers view to display a selected set of routers and their peer connections. From this view, you can then display information about peer routers, peer connections, and DLSw circuits. You can also view new nodes as they are added, and view the changing status of the devices and links dynamically.

Maps Applications

CiscoWorks Blue Maps offers both Motif-based and web-based network management applications for UNIX workstations.

Motif-Based Network Management Applications

CiscoWorks Blue Maps offers a set of network management applications that use the X Window System and Motif graphical interfaces to display graphical maps of the nodes and links in your network. Each application focuses on a particular protocol: DLSw, RSRB, or APPN/SNASw.

Web-Based Applications

CiscoWorks Blue Maps offers a set of web-based client/server applications that let you use web browsers to display information about RSRB, DLSw, and APPN/SNASw networks. The network information is presented in a tabular format. The web server runs on your Maps workstation and collects information from the Cisco routers in the network. You can use a web browser from any workstation in the network to connect to the web server to view the network.

Functions Common to Maps and SNA View

When you install the CiscoWorks Blue products, you always install all the code, whether you license maps, SNA View, or both. Maps and SNA View use many common functions:

- Share router database and SNA information
- Maintain the information in the database with the same set of processes, daemons, and commands:
  - Discovery processes
  - Polling processes
  - Host discovery processes
  - Web daemon for access to the CiscoWorks Blue database
- Monitor and control the common processes with the Process Manager
- Collect, log, and display error messages with the Message Logger
- Provide a graphical interface to discovery, creating key devices, and launching some of the main processes using the administration
- Allow access to the database information from the web using the same web server and web daemon
- Collect VTAM information at the mainframe and send it to the workstation

CHAPTER 2

Preparing to Install CiscoWorks Blue Applications

This chapter provides information on preparing to install CiscoWorks Blue Maps and SNA View on UNIX workstations.

This chapter includes the following main sections:

Hardware and Software Requirements for UNIX Workstations

This section lists the workstation requirements and Cisco IOS software requirements.

Workstation Software Requirements

CiscoWorks Blue Maps and SNA View run on the following systems:

- IBM RISC System/6000 workstation with AIX Version 4, Release 3.3 and Tivoli NetView for AIX Version 7.1
- HP 9000 series with HP-UX 11.0 and HP OpenView 6.1.
- SPARC workstation with Solaris 2.6 and, optionally, one of the following network management systems for event notification, automatic discovery, and trap collection:
  - Sun Solstice Site/SunNet/Domain Manager 2.3
  - Sun Solstice Enterprise Manager 2.0 with patch level 4
  - HP OpenView 6.1

Note Sun Solaris versions 7 and 8 and AIX Version 5.1 are not officially supported, but CiscoWorks Blue Release 3.0.1 has been tested on these versions successfully.

To enable CiscoWorks Blue on Solaris 7, set the following environment variable before starting the installation:
setenv INSTALL_SOL_27 TRUE

To enable CiscoWorks Blue on Solaris 8, set the following environment variable before starting the installation:
setenv INSTALL_SOL_28 TRUE

To enable CiscoWorks Blue on AIX 5.1, set the following environment variable before starting the installation:
setenv INSTALL_AIX_51 TRUE

CiscoWorks Blue and Network Management Systems

CiscoWorks Blue is not dependent on running with a network management system. The SNA View *dependency view* allows you to highlight a router and launch both CiscoView and CiscoWorks from that window. The programs run independently and do not share data.

Trap Processing

The network management systems offer some benefits in monitoring and improving performance. By receiving DLSw traps from the network management system, CiscoWorks Blue can update its database of DLSw peer and circuit status quickly if Cisco IOS is configured to send the traps to the network management system and the CiscoWorks Blue workstation. CiscoWorks Blue also takes the DLSw and SNASw traps and converts them into a more human-readable format and sends them back as traps to the local network management system. For example, CiscoWorks Blue displays MAC addresses and link names.

Discovery

CiscoWorks Blue preforms discovery by learning the routers discovered by the network management system and running its own discovery for DLSw, SRB, and TN3270. With this feature, users are not required to build a seed file of all of the routers that need to be managed.

Workstation Hardware Requirements

All platforms require the following hardware and software:

- Color monitor.
- PostScript-compatible printer (for printing window images).
- CD-ROM drive on the host system, or on an accessible remote host, for installation.
- Hard disk space—5 MB in the *var* partition, 500 MB in the */opt* file system for AIX or 250 MB for HP-UX and Solaris. If sufficient space is not available in */opt*, the installation program uses an alternate file system and creates symbolic links to */opt/CSCOcb*.
- RAM size—128 MB minimum (256 MB recommended).

- Swap space size—256 MB minimum or 1.5 times RAM size, whichever is greater.

Installation Authority Requirement

To install CiscoWorks Blue SNA View, you must have **root** authority on the machine you are installing the software.

Verifying UNIX Workstation Requirements

Table 2-1 lists commands that you can enter to verify hardware and software requirements on all platforms.

Table 2-1 Hardware and Software Verification Commands

Verify	On AIX	On HP-UX	On Solaris
Hard disk space	df -k	bdf	df -k
Operating system version	oslevel	uname -a	uname -a
NMS version	lslpp -L nv6000.base.obj	/usr/sbin/swlist | grep "Network Node Manager"	pkginfo | grep SNM /opt/OV/bin/ovversion
RAM size	lscfg | grep mem[1] lsattr -E -l mem0 -F "description value"[2]	/usr/sam/lbin/getmem	dmesg | grep mem
Swap space size	lsps -s	swapinfo	swap -s
X Window System version	Ask your system administrator.		

1. On an IBM RISC System 6000 workstation.
2. On a Power-PC workstation.

System Software Requirements

Your workstation must meet the following software requirements to run CiscoWorks Blue SNA View:

- X Window System Version 11, Release 5 with OSF/Motif Version 1, Release 2 (on UNIX servers only).
- Web Browser—Browser software is required to access the CiscoWorks Blue web interface and to see the online help for the Process Manager, Message Logger, and Administration programs:
  - Netscape Navigator 4.0 or later on Windows and UNIX systems, or
  - Microsoft Internet Explorer 4.0 or later on Windows systems only. Other web browsers may work, but have not been tested.

  Make sure JavaScript and cookies are enabled.
- Communication program—Either TCP/IP or LU 6.2 communications are required for connecting the CiscoWorks Blue workstation to a mainframe computer.
  - For LU 6.2 communications:
  - On AIX systems—IBM eNetwork Communications Server for AIX, Version 5.0
  - On HP-UX systems—HP-UX SNAplus2, including SNAplus2 Link and SNAplus2 API
  - On Solaris systems—Data Connection SNAP-IX V6.0.6 for SPARC For TCP/IP, you need the workstation operating system's TCP/IP package.

Sun Solaris Patch Requirements

The Solaris patches listed by version in this section are required for you to install Maps and SNA View. You can install these separately or as a jumbo patch from Sun Microsystems, Inc. To obtain the patches, contact your Sun Microsystems representative or download them from the Sun web site.

Solaris 2..6 Patches

The following minimum patch level is required on Solaris Version 2.6:

- Patch 105490-04 or later—Solaris 2.6 Linker patch

Required HP-UX Patches

HP suggests using the following 10 patches for using the jre on HP-UX. Without these patches, you can encounter a problem in which the jre runtime is unable to initialize. After you install the patches, the problem will be solved. After you install the patches, and the MsgLogClient starts, then the jre is working.

If your system already has a jre bundle installed, it may not require these patches and you can ignore them.

If you encounter a JRE initialization problem, you *must* install the following patches to solve the JRE initialization problem:

- PHCO_19666
- PHCO_20765
- PHCO_20882
- PHKL_18543
- PHKL_20016
- PHKL_20202
- PHCO_17058
- PHKL_19169
- PHKL_17038
- PHKL_20674

The HP-UX patches listed by version in this section are required for you to install Maps and SNA View. To obtain these patches, contact your Hewlett Packard representative.

Note Hewlett Packard often obsoletes old patches and incorporates their functions in new patches with different numbers. In the following sections, we list both the original patch we require and the latest patch, that we are aware of, that contains the required functions.

HP-UX 11.00 Patches

The following minimum patch levels are required on HP-UX Version 11.00:

- You must install PHSS_14577 (old) or PHSS_16587 (new) for HP 11.00, s700_800 11.00 HP C++ runtime library components (A.03.10).
- Cisco recommends that you install PHSS_16620 (old) or PHSS_18013 (new) for HP 11.00, X/Motif2.1 Runtime Nov98 Periodic Patch.

AIX Patches

The AIX patches listed by version in this section are required for you to install Maps and SNA View on AIX Version 4.3 or higher. To obtain the patches, contact your IBM AIX representative.

AIX 4.3

The following patches are required on AIX Version 4.3:

- bos.rte.libpthreads 4.3.0.2
- xlC.rte 3.6.6.0

Collecting Data for Installation on UNIX

During installation, you might be asked to provide information needed by the installation program, such as the locations of key programs or the identifications of ports to be used. You should collect the following information in advance to make the installation process easier.

Network Management System (NMS)

The installation program might ask for the directory path to an NMS, such as NetView for AIX, HP OpenView, or SunNet Manager. When one of these systems is found, the installation program can integrate CiscoWorks Blue applications with the NMS.

Netscape

The installation asks for the directory path and name of the Netscape executable program. Do not enter a Netscape shell script.

Port Numbers

The installation program assigns port numbers to several applications, including the port number used by the web server. If the default ports are unavailable, the installation program asks you for an available port number that it can assign.

CiscoWorks 2000

The URL for the CiscoWorks 2000 web page.

Domain name

Be prepared to supply a 1-8 character, uppercase domain name to identify your host connection.

Protocols

The installation needs to know which protocols are running in your network so that the appropriate programs can be set to start automatically (DLSw, RSRB, TN3270, and APPN/SNASw).

Seed files

If you will discover the network from seed files, you should carry over any seed files from previous installations.

License keys

Be prepared to enter the license keys for UNIX (one for Maps and one for SNA View).

APPN/SNASw topology agent name—This procedure is optional and applies to Maps only. After installation is complete, you might need to edit the *cwbinit* file or use the Configuration utility to enter the host name of the APPN/SNASw network topology agent.

Mainframe information

If TCP/IP is used between the mainframe and the workstation, the installation program needs the host name or TCP/IP address of the mainframe.

If LU 6.2 is used between the mainframe and the workstation, verify the basic LU 6.2 connectivity by using the following host command:
D NET,APING=NETID.CPNAME

Cisco IOS Software Requirements

For routers to be managed by CiscoWorks Blue Maps applications, all routers must be running a Cisco IOS release indicated below:

- For RSRB—Cisco IOS Release 11.0 or later. For FST transport, Cisco IOS Release 11.0(13) or 11.1(8) or 11.2(3) or later
- For DLSw—Cisco IOS Release 11.1(7) or later. For DLSw traps, Cisco IOS Release 11.3 or later
- For APPN/SNASw—Cisco IOS Release 11.0(6) or later. For DLUR, Cisco IOS Release 11.2(1) or later
- For SNA Switching Services—Cisco IOS Release 12.0(5)XN or Release 12.1 or later

Configuring Trap Destinations in Cisco IOS Routers

This section describes how to configure a router for use with CiscoWorks Blue Maps and SNA View. For detailed information about configuring the Cisco IOS software with the **snmp-server** command, see the C*isco IOS Configuration Fundamentals Command Reference*. The following trap configuration methods are described in this section:

- Configuring Traps in RSRB-Enabled Routers, page 2-10
- Configuring Trap Destinations in DLSw- and RSRB-Enabled Routers, page 2-11
- Configuring Trap Destinations for SNASw- and DLSW-Enabled Routers, page 2-12

Configuring Cisco IOS Software in Managed Routers

Configure the Cisco IOS software in every managed router using the following command:

snmp-server community *string* **RO**

Where:

string is the community string (a password for access to SNMP) in this router.

RO specifies read-only access to SNMP in this router.

Configuring Traps in RSRB-Enabled Routers

For the trap daemon (cwbtrapd) to perform optimally for RSRB, all RSRB-enabled routers must specify their addresses in the traps that they generate. Therefore, you must configure the Cisco IOS software in every RSRB-enabled router using the following command:

snmp-server trap-source *interface*

Where:

interface specifies the router interface (such as tokenring1) whose IP address is used as the local address for RSRB peering and is stamped on the traps that this router generates.

Note The information in this section applies to Ciscoworks Blue only if you are running a UNIX workstation with an NMS during an installation.

Configuring Trap Destinations in DLSw- and RSRB-Enabled Routers

To use router-generated traps, all DLSw- and RSRB-enabled routers must specify the CiscoWorks Blue Maps network management host as the destination of DLSw and RSRB traps. Therefore, you must configure the Cisco IOS software in every DLSw- and RSRB-enabled router.

Note The information in this section applies to Ciscoworks Blue only if you are running a UNIX workstation with an NMS during an installation.

To configure a DLSw router, use the following command:

snmp-server host *address string* **dlsw**

Where:

address is the IP address of the network management host, such as 123.45.67.89.

string is the community string for access to SNMP in the network management host.

dlsw limits the traps sent to DLSw-related traps.

To enable the DLSw traps, use the following command:

snmp-server enable traps dlsw [circuit | tconn]

Where:

circuit limits the traps to DLSw circuit-related traps.

tconn limits the traps to DLSw peer-related traps.

To configure an RSRB router for traps, use the following command:

snmp-server host *address string* **rsrb**

Where:

address is the IP address of the management host, such as 123.45.67.89.

string is the read community string for access to SNMP in the management host.

rsrb sends only RSRB-related traps to *address*.

Configuring Trap Destinations for SNASw- and DLSW-Enabled Routers

If Cisco IOS is not configured to send traps to the CiscoWorks Blue workstation, when CiscoWorks Blue detects DLSw and APPN/SNASw resource changes, it will send traps to the local network management system to notify the operator of the state changes. However, if Cisco IOS is configured to send CiscoWorks Blue traps, then only those traps will be seen and not the existing traps.

CiscoWorks Blue receives Cisco IOS traps for DLSw encapsulation and APPN/SNASw, converts them from hexadecimal to a human-readable format and sents them back to OpenView, NetView, or SunSolstice.

To take advantage of this trap conversion, you must configure SNASw and DLSw routers to send Cisco IOS traps to the CWBlue workstation.

Enable SNASw traps with the following configuration command:

```
Hardy(config)#snmp-server enable traps snasw ?
  cp-cp     Enable SNMP snasw local topology tg cp-cp session traps
  dlus      Enable SNMP snasw dlus traps
  isr       Enable SNMP snasw intermediate sessions traps
  link      Enable SNMP snasw link traps
  port      Enable SNMP snasw port traps
  topology  Enable SNMP snasw local topology tg traps
  <cr>
```

For information about specific traps and their corresponding conversions, see Chapter 10, “Event Notification Messages”.

Setting Kernel Parameters on HP-UX Systems

If you install the CiscoWorks Blue applications on an HP-UX system, you might need to change the following kernel parameters. Use the HP-UX **sam** command to change the kernel parameters if they are lower than the following settings:

- max_thread_proc—1024
- ncallout—2040
- nfile—3000
- ninode—1900
- nkthread—18848
- nproc—664
- semmni—512

See your HP-UX publications for instructions on changing these values.

These values are the minimum values needed for Maps and SNA View. If you have other resource-intensive applications on this workstation, you might need to increase these values. If you are unable to start the Process Manager, if you get “out of space” errors while trying to start other CiscoWorks Blue processes, or if you get Java exceptions with the message “out of memory,” try increasing the swap space.

Becoming the Root User

Before you install CiscoWorks Blue Maps or SNA View on UNIX workstations, you must have root user authority. The user named root can perform functions restricted from normal users. You can log in to your system as the root user, or you can become the root user by using the **su** command. You will then be asked to enter the root user’s password.

Caution If you are a relatively inexperienced UNIX user, limit your activities as the root user to the tasks described in this publication. As the root user, you can adversely affect your operating environment if you are unaware of the effects of the commands that you use.

If you are not logged in, you can log in as the root user by responding to the login prompt with the username **root**.

```
login: root
Password: rootpassword
```

If you are already logged in, but not as the root user, use the **su** command to become the root user:

% **su**

```
Password: rootpassword
```

Using Key Devices

This section describes how you can specify selected DLSw routers as key devices to limit some of the SNMP traffic on your network.

A key device is a router that you designate as "key." This means that the router is in close proximity to the mainframe, or it supports an important set of network resources. You can use key routers to reduce the SNMP traffic needed to manage your network, to minimize the number of devices shown on a DLSw map, and for circuit polling, which is needed for SNA correlation. You can also specify a faster polling rate for key devices.

Reduce SNMP Traffic

You can limit some of the SNMP traffic involved in discovering and polling routers by selecting only key routers that are in close proximity to the mainframe and that are responsible for handling traffic between the mainframe and other remote routers and devices in your network. If a router is marked as a key device,

the poller daemon polls this router for all of the circuits in addition to the peer connections. If a router is not marked as a key device, the poller daemon polls the router for the peer connections.

A DLSw circuit is represented in both of the DLSw peers through which an SNA session passes. Because part of the circuit information is duplicated in each peer router, the DLSw Maps application can find the SNA path used, even if it polls only one of the routers (a key router, for example). Polling one peer reduces the polling interval and reduces network traffic.

Minimize Displayed Devices

If you designate a set of routers as key devices, you can later display a view of just the key devices. This view is called the key devices view of the network and is described in the *CiscoWorks Blue Maps and SNA View User Guide*.

The key devices view of the network displays just the DLSw-enabled peer routers that are designated as key devices. The key devices view represents all the peers of a key router with one icon, which is called an aggregated peer router icon. The connection between each key router and its aggregated peer router icon is shown as a single connection called an aggregated peer connection.

To see how using key devices removes the clutter from your maps, compare the key devices view with the global view shown in the *CiscoWorks Blue Maps and SNA View User Guide*.

Optimize Polling

The DLSw application lets you define polling intervals. See the “Using the cwbinit File” section on page 4-12.

You can specify how the DLSw application polls routers for peer connection information and for circuit information. You can select from the following polling methods:

- The Key-Peer polling method polls only key routers for peer connection information. You might set this interval so that key routers are polled more frequently.
- The Non-Key-Peer polling method polls only the non-key routers for peer connection information. These routers can be polled less frequently.

- The Key-Circuit polling method polls only the key routers for circuit information.

If you make no changes, the DLSw polling daemon uses all three polling methods: It polls key routers and non-key routers for peer connection information, and it polls key routers for circuit information. You can change these selections using the polling values in the *cwbinit* file.

You can also use the *cwbinit* file to configure multiple polling threads. By default, Key-Peer polling uses five threads so that it can poll more key routers concurrently, while Non-Key-Peer polling uses only one thread by default. You can change these settings in the *cwbinit* file.

Choose Key Routers

This section gives you guidance in choosing which routers to designate as key devices. Usually, you want to choose key routers for the following reasons:

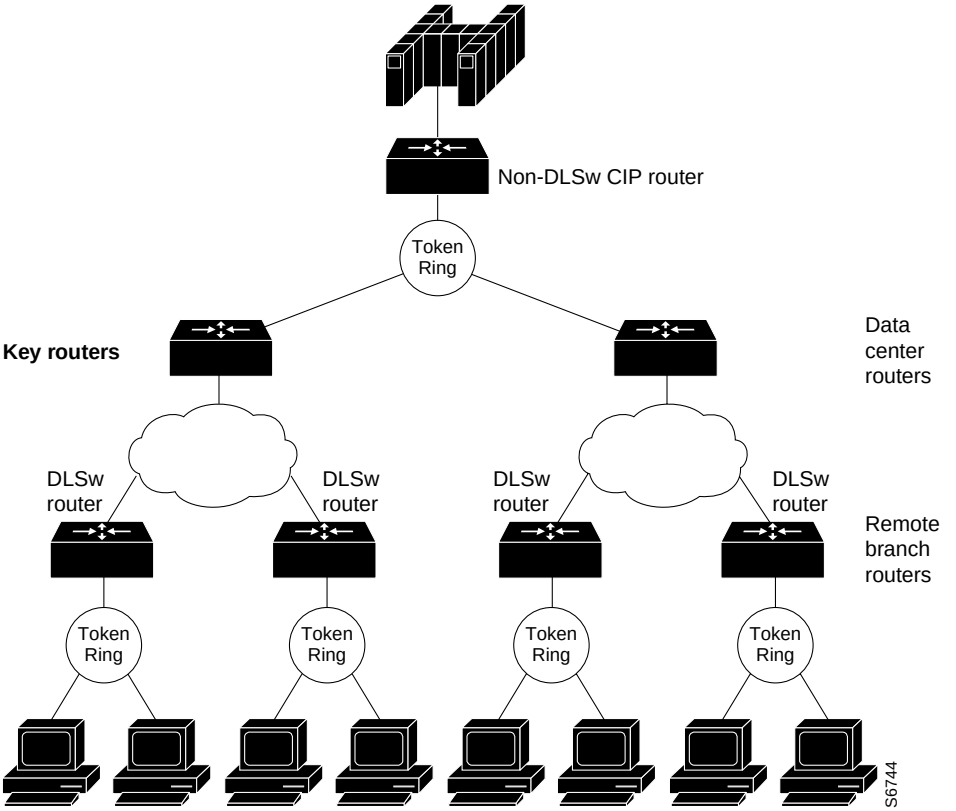
- They are near the mainframe.
- They support a large or important set of network resources.
- They support the largest number of peer connections and circuits.

The following two network examples show how to choose key routers.

Data Center Routers Example

Figure 2-1 shows a network in which the two DLSw-enabled data center routers handle all the peer connections between the mainframe and the remote branch routers. In this case, you should designate these two data center routers as key devices.

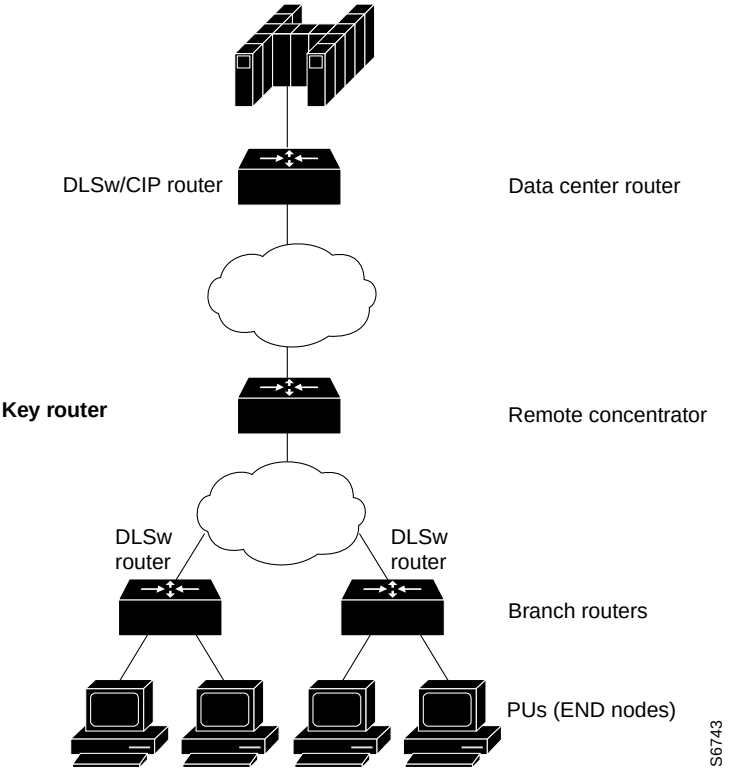
Figure 2-1 Example1: Data Center and Remote Branch Routers



Concentrator Router Example

Figure 2-2 shows a network in which one DLSw-enabled concentrator router handles all the connections between the mainframe and the remote branch routers. In this case, you should designate the concentrator router as a key device.

Figure 2-2 Example 2: Concentrator and Remote Branch Routers



Define Key Devices

Initially, no routers are marked as key devices when they are added to the database. You must take some action to mark a router as a key device. You can define a router as a key device by using

- a seed file
- the Edit menu

Defining Key Devices Using the Seed File

For each router that you include in the seed file, you can use the key parameter to designate that router as a key device. If the key parameter is not used, the router is not a key device in the seed file. To see which routers are key devices, select **Edit > Key Device(s)** from the menu bar on the Motif application. In the list of routers, the key devices are highlighted.

Once you mark a router as a key device, removing the key parameter in the seed file will not change the device's status as a key device. To change the router's status as a key device, select **Edit > Key Device(s)** from the menu bar on the Motif application, deselect the router in the router list, and click **Apply**.

Defining Key Devices Using the Edit Menu

You can select the **Key Device(s)** menu item from the DLSw Edit menu on the Motif application to define routers as key devices. If you designate several routers as key devices, you can later display a key devices view of the network, as described in the *CiscoWorks Blue Maps and SNA View User Guide*. The following procedure describes how to use the Edit menu to define a key device:

Step 1 From the DLSw menu bar on the Motif application on UNIX workstations, select **Edit > Key Device(s)**. A list of routers is displayed. If a router name is highlighted, it is a key device.

Step 2 Select those routers that you want to add to the list of key devices. Each router that you select is highlighted.

Step 3 Deselect those routers that you do not want to be key devices. The routers that you select here will not be highlighted.

Step 4 Click **Apply** to apply your changes in the database.

Step 5 Click **Close** to close the window.

CHAPTER 3

Installing and Configuring CiscoWorks Blue

This chapter provides information on installing and configuring CiscoWorks Blue Maps and SNA View on AIX, HP-UX, and Solaris workstations.

This chapter includes the following main sections:

Note Refer to the *Release Notes for CiscoWorks Blue Maps and SNA View Software Release 3.0.1* for cautionary statements about the installation and configuration process. Also review the "Collecting Data for Installation on UNIX" section on page 2-7.

Upgrading to CiscoWorks Blue Release 3.0.1

This section describes how to upgrade to CiscoWorks Blue Maps or SNA View Release 3.0.1 from a previous release.

Creating a Seed File from a Previous Software Release Database

Use the following procedure to create a seed file from your database of a previous release for use with your Release 3.0.1 applications.

Note You can avoid having to discover the network from the network management database by creating a seed file or saving the seed file from the previous release.

Creating a Seed File in a Previous Release

Enter the following command:

cwb create seed [**-s** *seedfile*]

Where **-s** *seedfile* specifies the name of the seed file to create. If you omit this parameter, the seed file is named *seed.file*.

Note When you deinstall CiscoWorks Blue, the following configuration files are saved in the */var/tmp/cwb.save* directory: *cwbinit*, *runprocess*, *CWBlue.conf*, *Services.conf*, and *SeedFile*.

Upgrading SNA View Configuration Files

If you specify the same domain name during configuration of Release 3.0.1, your mainframe connection configuration file will be upgraded automatically.

Using CiscoWorks Blue Release 3.0.1 Workstation Software with a Previous SNA View Release of Mainframe Software

If you are installing CiscoWorks Blue Release 3.0.1, the mainframe software must be at least Release 2.1 (version 3.0 for LU 6.2 users). Cisco strongly recommends that you upgrade both the mainframe software and CiscoWorks Blue to Release 3.0.1.

Note If you plan to connect a workstation running CiscoWorks Blue Release3.0.1 to a mainframe running a previous release of SNA View using TCP/IP, set MESSAGES OFF in the NSPPARM file on the mainframe to avoid connectivity problems.

Saving the cwbinit File

Before you install CiscoWorks Blue Release 3.0.1, you might want to save the *$CWBROOT/etc/cwbinit* configuration file from your previous release. Although the previous versions of this file are not suitable for use with Release 3.0.1, you can copy settings from the older release after you install Release 3.0.1.

Deinstalling Maps and SNA View from a Previous Release

Before you install CiscoWorks Blue Maps and SNA View Release 3.0.1, you must deinstall the previous release. Use the deinstall script from the CD-ROM to perform the deinstall function.

Use the instructions in the “Deinstalling CiscoWorks Blue From a Previous Release” section on page 3-46

Installing and Configuring CiscoWorks Blue

You can install and configure CiscoWorks Blue Maps and SNA View from a local or remote CD-ROM drive. In either case, you install both Maps and SNA View at the same time. The license that you purchase from Cisco determines which applications you can use. You must have a license key for each application, one for Maps and one for SNA View.

This section includes the following subsections:

If it is necessary to reinstall a CiscoWorks Blue product, deinstall the existing software using procedures in the "Deinstalling CiscoWorks Blue From a Previous Release" section on page 3-46, and then reinstall as if it were a new installation.

Installing CiscoWorks Blue Maps and SNA View

Use the following procedure to install the software on your system. The default for each prompt is the value in brackets. To accept any default value, press **Enter**.

Installing from a Remote CD-ROM Drive

If you are installing from a remote CD-ROM drive, insert the CD-ROM into the drive on a remote system and export the CD-ROM file system (make it available to an outside system). If you are installing from a local CD-ROM drive, insert the CD-ROM in the drive on the local system, then mount the CD-ROM file system on the local system. If you do not know how to mount a CD-ROM drive from a local or remote system, see Appendix B, "Mounting a CD-ROM on UNIX Workstations."

Installing from a Remote System

If you are installing from a remote system, you must export your display to that remote system to view the applications that are started at the end of the installation process.

Installing the First CiscoWorks Blue for the First Time

If you are just now installing your first CiscoWorks Blue 3.0.1 product, go to the "Installing the CiscoWorks Blue 3.0.1 Products."

Installing a Second CiscoWorks Blue Product

If you have already installed one of the CiscoWorks Blue 3.0.1 products, either Maps or SNA View, and now want to install the other CiscoWorks Blue 3.0.1 product, *do not* go through the installation process. Instead, apply the second license key to the license file, as described in the "Applying Licenses after Installation."

Installing the CiscoWorks Blue 3.0.1 Products

The default for each prompt is the value shown in brackets. To accept any default value, press **Enter**.

Step 1 Before you start, collect the necessary information as described in the "Collecting Data for Installation on UNIX" section on page 2-7.

Step 2 If you have any release of CiscoWorks Blue Maps or SNA View installed, deinstall it as described in the "Deinstalling CiscoWorks Blue From a Previous Release" section on page 3-46 or the "Modifying Color Schemes for the Maps Motif Applications" section on page 3-47 before you begin to install CiscoWorks Blue Maps or SNA View Release 3.0.1.

Note When you deinstall a previous release and then install Release 3.0.1, the following configuration files are saved in the */var/tmp/cwb.save* directory for reference: *cwbinit*, *runprocess*, *CWBlue.conf*, *Services.conf*, and *SeedFile*.

Step 3 Start the interactive installation script by entering the following command:

/cdrom/setup.sh

Step 4 If you have already installed the products and are already licensed for Maps but not for SNA View, you will see the following message.

```
INFO:Your current CiscoWorks Blue SNA View license key is not valid.
Do you want to enter CiscoWorks Blue SNA View license key[yes|no]? [Y]
```

Press **Enter** to install a license for SNA View.

- If you enter **Y**, go to the "Applying the CiscoWorks Blue Licenses" section on page 3-11.
- If you enter **N**, installation stops.

Step 5 If you have installed the products and are already licensed for SNA View and not for Maps, you will see the following message:

```
INFO:Your current CiscoWorks Blue Maps license key is not valid.
Do you want to enter CiscoWorks Blue Maps license key[yes|no]? [Y]
```

Press **Enter** to install a license for Maps.

Step 6 If you have installed the products but you have applied a temporary license key for an evaluation copy of Maps or SNA View, or a license key that is invalid, you might see one of the following messages:

```
INFO:Your current CiscoWorks Blue Maps license expires on mm/dd/yyy.
Do you want to enter CiscoWorks Blue Maps license key[yes|no]? [Y]

INFO:Your current CiscoWorks Blue SNA View license expires on
mm/dd/yyy.
Do you want to enter CiscoWorks Blue SNA View license key[yes|no]? [Y]

INFO:Your current CiscoWorks Blue Maps license key is not valid.
Do you want to enter CiscoWorks Blue Maps license key[yes|no]? [Y]

INFO:Your current CiscoWorks Blue SNA View license key is not valid.
Do you want to enter CiscoWorks Blue SNA View license key[yes|no]? [Y]
```

Press **Enter** if you now want to apply a valid, permanent license key for Maps or SNA View.

Step 7 If you have already installed the products but did not apply any license, and then you reran the installation program, you will see the following message:

```
INFO:Your current CiscoWorks Blue license keys are not valid.
Do you want to enter CiscoWorks Blue license key(s) [yes|no]? [Y]
```

Press **Enter** to install a license.

Step 8 The setup program starts and displays the following banner:

```
**********************************************************************
*                           Cisco  Systems
*      .          .                                  .          .
*      |          |          CiscoWorks             |          |
*     :|:        :|:      Blue Maps and SNA View  :|:        :|:
*   :|||||:    :|||||:                           :|||||:    :|||||:
* .:|||||||:..:|||||||:.    Setup  Program     .:|||||||:..:|||||||:.
**********************************************************************
```

Note Installation error messages are self-describing and are not described in this manual. If you cannot complete the installation successfully, call the Cisco TAC.

Step 9 On Solaris, if you have more than one network management system (NMS) installed, select which NMS you want to integrate with CiscoWorks Blue. The installation program detects if you have any network management systems installed. If it finds more than one NMS, it asks you to select one to use. In response to the following prompt, type **SNM** to use the Sun Net Manager, or type **HPOV** to use HP-OpenView.

```
INFO: Install program detected SunNet Manager and HP Openview
installed on the machine.
Which NMS platform do you want to use to integrate CiscoWorks Blue
Product?: [SNM/HPOV]
```

Step 10 If the installation program cannot find an NMS, either enter the NMS path or specify no **NONMS**:

- On Solaris systems:

  In response to the following prompt, specify which NMS is installed:

  ```
  Install program did not detect either HP OpenView or SunNet
  Manager
  Do you have either HP OpenView or SunNet Manager installed on the
  system? [HPOV/SNM/NONMS]
  ```

  - Type **HPOV** if HP OpenView is installed.
  - Type **SNM** if SunNet Manager is installed.
  - Type **NONMS** if no NMS is installed.

- On HP systems:

  In response to the following prompt, specify which NMS is installed:

  ```
  Install program did not detect HP OpenView
  Do you have HP OpenView installed on the system? [HPOV/NONMS]
  ```

  - Type **HPOV** if HP OpenView is installed.
  - Type **NONMS** if no NMS is installed.

- On AIX systems:

  In response to the following prompt, specify which NMS is installed:

  ```
  Install program did not detect NetView for AIX
  Do you have NetView for AIX installed on the system? [NETV/NONMS]
  ```

  – Type **NETV** if NetView for AIX is installed.

  – Type **NONMS** if no NMS is installed.

Step 11 And, in response to the next prompt, enter the full path name for the NMS:

- For SunNet Manager:

  ```
  Enter the SunNet Manager installation root directory:
  ```

- For HP OpenView:

  ```
  Enter the HP OpenView installation root directory:
  ```

- For NetView for AIX:

  ```
  Enter the NetView for AIX installation root directory:
  ```

Step 12 In response to the following prompt, enter the path and name of your Netscape browser binary file (the executable file):

Note This file should be the Netscape executable, not a shell script that runs Netscape.

```
Enter fully qualified Netscape browser executable path
```

Type the full path (including filename) to the Netscape browser binary file; for example:

```
Enter fully qualified Netscape browser executable path
/usr/local/packages/cnetscape/current/Solaris-2.5/netscape.128
```

If you do not have Netscape installed yet, you can install it later. At that time, add the string *Netscape* to your path statement and ensure that the Netscape executable name is *Netscape*.

Step 13 (Optional) If you are installing on a Solaris platform and want to use the path tool for mainframes in HPR/IP session paths, "traceroute" must be included in your current path. If "traceroute" is not in your current path, you will be prompted to supply the path as in this example:

```
Ener fully qualified traceroute executable path
```

Type the full path of the **traceroute** command.

To skip this step, hit the **Enter** key.

Step 14 In response to the following prompt, press **Enter** to accept the default or enter a new path for installing the product. Normally the installation program chooses the drive with space available.

```
Where should the product be installed? [/opt]
```

Note The installation program always creates links from */opt/CSCOcb* to wherever you choose to install the product. You can always find the CiscoWorks Blue **cwb** command in */opt/CSCOcb/bin*.

Step 15 For AIX systems, if there is insufficient room in the */usr* file system, in response to the following prompt, press **Enter** to expand the */usr* file system:

```
/usr has insufficient space for installation.
Do you want to expand /usr partition [yes|no]? [Y]
```

Step 16 The program installs the software from the CD-ROM and reports on its progress.

You can use the **more** command to examine the installation log file for error messages.

```
more /opt/CSCOcb/install/cwb_install.log
```

Press the **Spacebar** to advance the display one screen at a time.

When installation is complete, the *cwbinit* script is added to the system initialization files to automatically start the CiscoWorks Blue processes when you reboot.

This concludes the installation process. Go to the next section to apply your licenses for CiscoWorks Blue applications.

Applying the CiscoWorks Blue Licenses

During installation, you can apply the license information for the Maps and SNA View applications. If you do not apply the license information now, you can apply it later as described in the "Applying Licenses after Installation" section on page 3-43.

Note If you uninstalled CiscoWorks Blue Release 3.0 from the Release 3.0.1 CD, your licenses will be automatically restored. Depending on which products you had previously licensed, Steps 1 and 2 in this procedure will be skipped.

Step 1 In response to the prompt, enter the Maps license key as found in your license materials**.** If you are not licensed for Maps, press **Enter**.

```
Enter the CiscoWorks Blue Maps license key (example:123456789012) or
press enter if not licensed for CiscoWorks Blue Maps
```

Step 2 In response to the following prompt, enter the SNA View license key as found in your license materials. If you are not licensed for SNA View, press **Enter**.

```
Enter the CiscoWorks Blue SNA View license key (example:123456789012)
or press enter if not licensed for CiscoWorks Blue SNA View
```

Step 3 In response to the prompt, press **Enter** to configure the installed product now and go to the next section. If you enter **N**, you can configure the product later using the **cwb config** command.

```
Would you like to configure CiscoWorks Blue Maps now [yes|no]? [Y]
```

Go to the next section to configure CiscoWorks Blue applications.

Configuring CiscoWorks Blue

After you install Maps and SNA View, configure the application using the following procedures.

- Specify an SNA domain name and protocol for a connection to an SNA mainframe.
- Specify the protocols (DLSw, APPN/SNASw, RSRB, and TN3270) to be managed so that the Process Manager sets up the correct processes.
- Specify whether to query a domain name server (DNS) for router host names.
- Specify the ports to use for CiscoWorks Blue processes.

Note If you do not configure now, you can use the **/opt/CSCOcb/bin/cwb config** command to configure later.

Using Default Values

In the configuration procedure, the default for each prompt is the value shown in brackets. To accept any default value, press **Enter**.

The CiscoWorks Blue configuration procedure starts with a set of predefined default values. After you run the CiscoWorks Blue configuration procedure the first time, the choices you make become the default values for the next time you run the program. For example, the first time you run the program, the default for enabling DNS queries is **N**:

```
Would you like to enable DNS search [yes|no]? [N]
```

If you change the **N** to **Y** and press **Enter** to enable DNS queries, the next time you run the configuration procedure, the default changes to **Y**:

```
Would you like to enable DNS search [yes|no]? [Y]
```

Note In the prompts in the following section, the values shown in brackets are the predefined default values used when you first run the configuration program.

Using the Configuration Procedure

The installation script should automatically start the configuration script. If it does not, or if you want to reconfigure the product at any time, you can start the interactive configuration script with the **cwb config** command as described in the "Configuring CiscoWorks Blue after Installation" section on page 3-45.

Note You must have applied a valid Maps or SNA View license to configure the product.

Use the following information to configure the CiscoWorks Blue:

Step 1 In response to the following prompt, type **Y** and press **Enter** to configure the mainframe connection now or type **N** and press **Enter** to bypass configuring a mainframe connection. You can use the **cwb confi**g command later to configure a mainframe connection.

```
Would you like to Add/Modify/Delete a SNA host connection [yes|no]?
[Y]
```

Step 2 At the following prompt, enter the name of the mainframe SNA domain in uppercase letters:

```
SNA Domain name(s) (Use upper case letters only):MVSD
```

To specify a domain name, enter any 1- to 8-character alphanumeric value. Choose a name that is meaningful in your environment, such as an SSCP name or host PU name. This domain name is added as an extension to all PU and LU names to create the format PUNAME.DOMAIN, which is used in the SNA View database and on the Maps views. You must use all uppercase characters in domain names.

Step 3 To reconfigure an existing domain, specify an existing domain name. The configuration program displays a message informing you of the reconfiguration of the existing file. Type **Y** and press **Enter** to modify the selected mainframe connection now or type **N** and press **Enter** to bypass modifying the mainframe connection.

```
Would you like to modify it [yes|no]? [Y]
```

You might want to reconfigure an existing domain if you migrated configuration files from a previous release of SNA View.

Step 4 At the following prompt, specify whether the connection to that domain is using LU 6.2 or TCP/IP. Type **TCP** and press **Enter** to configure a TCP/IP connection or type **LU62** and press **Enter** to configure an LU 6.2 connection.

```
Connectivity to mainframe (TCP or LU62): TCP
```

If you enter TCP, then the Process Manager automatically starts the *cwbhcid* daemon to start a connection to the mainframe component.

At this point in the configuration process, if your host connection is via LU 6.2, you should configure the host connection as described in the "Configuring the Host Connection" section on page 3-24.

Step 5 At the following prompt, for TCP/IP connections only, enter the TCP/IP address or host name for the SNA mainframe:

```
Mainframe TCP/IP Name or Address: rtpmvsd
```

For each SNA domain that you configure, the program builds a configuration file named */etc/svopen_config_DOMAINNAME*, where *DOMAINNAME* is the name of the SNA domain that you specified. To review the SNA parameter values, edit this file as described in the "Configuring Domain-Specific Parameters" section on page 3-24.

Note The configured mainframe ports for */etc/svopen_config_hostname* are 6104 and 6105. Ensure that *NSPPARM* on the mainframe is configured to match. See the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide* for more information.

Step 6 When you see the following prompt, type **Y** and press **Enter** to configure another host domain or type **N** and press **Enter** to stop configuring host domains.

```
Configure another SNA host connection [yes|no]? [N]
```

Step 7 In response to the following prompt:

- Type **Y** and press **Enter** to specify that you manage APPN/SNASw. This action makes *cwbsnamapsd* dependent on AppnPollerServer in the Process Manager and is used by **cwb verify** to check for valid configuration.
- Type **N** and press **Enter** to specify that you do not manage APPN/SNASw.
- Press **Enter** to accept the default.

```
Configure APPN [yes|no]? [Y]
```

Step 8 In response to the following prompt:

- Type **Y** and press **Enter** to specify that you manage DLSw. This action makes *cwbdlswpollerd* and *cwbtrapd* (if an NMS is present) start automatically in the Process Manager and is used by **cwb verify** to check for valid configuration.
- Type **N** and press **Enter** to specify that you do not manage DLSw.
- Press **Enter** to accept the default.

```
Configure DLSW [yes|no]? [Y]
```

Step 9 In response to the following prompt:

- Type **Y** and press **Enter** to specify that you manage RSRB. This action makes *cwbrsrbpollerd* and *cwbtrapd* (if an NMS is present) start automatically in the Process Manager and is used by **cwb verify** to check for valid configuration.
- Type **N** and press **Enter** to specify that you do not manage RSRB.
- Press **Enter** to accept the default.

```
Configure RSRB [yes|no]? [Y]
```

Step 10 In response to the following prompt:

- Type **Y** and press **Enter** to specify that you manage TN3270.
- Type **N** and press **Enter** to specify that you do not manage TN3270.
- Press **Enter** to accept the default.

```
Configure TN3270 [yes|no]? [Y]
```

Step 11 In response to the following prompt:

- Type **Y** to specify that you do want a DNS lookup when devices are added to the database. Press **Enter**.
- Type **N** to specify that you do not want a DNS lookup when devices are added to the database. Press **Enter**.
- Press **Enter** to accept the default.

Note The option you select here is used to set the *doDNSSearch* variable in the *cwbinit* file.

If you select **N**, then a device can be added only by the name with which the device was discovered. If you select **Y**, then a DNS lookup will let you enter any other valid names for the device that can be resolved by a DNS. For example, using DNS lookup, a device that was discovered as *heritage.cisco.com* could also be referred to as *heritage*.

```
Devices in the network may be referred to in different ways. For
example a device may be discovered as router1.cisco.com, but a
Maps/SNA View user may refer to the device just as router1. In order
for the application to identify both names as the same device it
must perform a DNS lookup on the device name both when it is
discovered and for each client request that can not be identified
based upon the device name supplied. Enabling DNS searches can
increase the device discovery time and the amount of time it takes to
service requests, especially if the DNS searches fail for the devices
being discovered.

Would you like to enable DNS search [yes|no]? [N]
```

Step 12 In response to the following prompt, press **Enter** to accept the default port for use by the CiscoWorks Blue web server or type in another TCP port above 1023 and press **Enter**. Initially, the default port is port 80.

```
Enter 80, 8080 or an unused tcp port above 1023 for Web Server:[80]
```

The configuration program checks to see whether the selected port is available. If it is unavailable, you will be prompted to select another port for the web server.

Step 13 In response to the following prompt, press **Enter** to accept the default port for use by the CiscoWorks Blue Open Server Gateway or type in another TCP port above 1023 and press **Enter**. Initially, the default port is port 44541.

```
Enter an unused tcp port above 1023 for Open Server Gateway:[44541]
```

The configuration program checks to see whether the selected port is available. If it is unavailable, you will be prompted to select another port for the Open Server Gateway.

Step 14 In response to the following prompt, press **Enter** to accept the default port for use by the CiscoWorks Blue Name server or type in another UDP port above 1023 and press **Enter**. Initially, the default port is port 44542.

```
Enter an unused udp port above 1023 for Name Server:[44542]
```

The configuration program checks to see whether the selected port is available. If it is unavailable, you will be prompted to select another port for the Name server.

Note Ensure that the ports that you select are not used by other applications. During configuration, the */etc/services* file and current ports in use are checked, but a service might not be active at the moment. If you need to change this port later, you must reconfigure the product using the **cwb config** command.

Step 15 If one of the selected ports is reserved in the */etc/services* file but does not appear to be in use at this time, you might see the following message. If you want to keep the port reserved and use another port, type **N** and press **Enter**.

```
WARNING: Port port_number/protocol is reserved for application_name
service in /etc /services file.
Do you want to use port_number/protocol anyway [yes|no]? [N]
```

Step 16 In response to the following prompt, type **Y** and press **Enter** to stop and restart CiscoWorks Blue processes or type **N** and press **Enter** to restart them at a later time. If you make any changes to the CiscoWorks Blue configuration, you must stop and restart all CiscoWorks Blue processes before those changes become active.

You will see this prompt only if you have configured the product already and are now changing that configuration.

```
CiscoWorks Blue configuration has changed. You must restart
all CiscoWorks Blue processes to make these changes effective.
Do you want to restart CiscoWorks Blue processes [yes|no]? [Y]
```

This concludes the configuration process. To start CiscoWorks Blue processes, go to the "Enabling DNS Lookups for Device Queries" section on page 3-17.

Enabling DNS Lookups for Device Queries

When CiscoWorks Blue processes add a device to the database or make device queries, they use the device host names. If a DNS is available, the processes can query the DNS to resolve the host names. If a DNS is not available, the processes must use the exact device names with which the devices were first discovered.

If you do not enable DNS queries, a device can be added only by the name with which the device was discovered. If you enable DNS queries, a DNS lookup will let you enter any other valid names for the device that can be resolved by a DNS. For example, using DNS lookup, a device that was discovered as *heritage.cisco.com* could also be referred to as *heritage*.

Use the following sections for information on selecting DNS lookup:

- Selecting DNS Lookup During Configuration, page 3-18
- Selecting DNS Lookup with the doDNSSearch Variable, page 3-18

Selecting DNS Lookup During Configuration

During configuration, a prompt asks you to specify whether or not to use a DNS lookup when devices are added to the database.

Selecting DNS Lookup with the doDNSSearch Variable

The *doDNSSearch* variable in the *cwbinit* file lets you specify to use DNS lookup to query routers during discovery and polling. In previous releases, you had to enter the exact name of the router by which it was first discovered. You can set this variable so that you can enter a different host name that can be resolved by a DNS lookup. This variable is used when you do the following:

- Discover devices with the Maps and SNA View web interface
- Use the Administration program to discover, rediscover, and add devices
- Use the **cwb start cwbdiscover** command
- Use discovery or add devices in the Maps Motif application

The following new section of the *cwbinit* file provides the *doDNSSearch* variable:

```
# This boolean value is used by both the cwbsnamapsd server process
# and other processes such as cwbadmin, cwbdiscover, dlsw and rsrb
# that add devices to the database.
#
# When adding a device to the database, this value is used to decide
# whether to do a DNS lookup on the name of the device being added,
# storing the DNS name in the DNS database table.
#
# cwbsnamapsd uses this value to decide whether to do a DNS lookup on
# a device name supplied in a user's request, if the request could
# not be satisfied with a device name or IP address lookup.
#
# The default value is "false", DNS lookups are not enabled. Set this
# value to "true" to enable DNS lookups.

doDNSSearch = false
```

Note You can set the *doDNSSearch* value during configuration.

You can set the *doDNSSearch* variable in the *cwbinit* file to **true** to discover and query routers by any valid name. Now you can enter the discovered name, a valid IP address, or any valid name for the router. For example, you could enter **cwb-c5** in the input field for a DLSw focus view even if the router was discovered as *cwb-c5.cisco.com*. To enable DNS lookup for routers, change the doDNSSearch value to **true**:

```
doDNSSearch = true
```

The DNS lookup is done when the router is added to the database and any time a device cannot be found by the discovered name or IP address. This search might impact performance.

Note After you change the *doDNSSearch* parameter, you should stop and restart *cwbsnamapsd*.

Starting the CiscoWorks Blue Processes

This section describes how to start CiscoWorks Blue processes during installation.

Step 1 In response to the following prompt, press **Enter** to start the CiscoWorks Blue servers. If you enter **N**, you can start the servers yourself with the **cwb start servers** command, as described in Chapter 4, "Monitoring and Controlling CiscoWorks Blue Applications."

```
Would you like to start the CiscoWorks Blue Maps processes now
[yes|no]? [Y]
```

Step 2 When the servers are started, the installation program displays the current status of all CiscoWorks Blue servers and processes:

```
CiscoWorks Blue Naming Server Started.
CiscoWorks Blue Process Manager Started.
Process Manager running with processes:

PROCESS              STATE    PID        Last Message
CWBHTTPAdapter       Ready    45818      Running
CWBOSAMonitor        Ready    25078      Running
cwbhcid_MVSDTCP      Ready    26162      Running
    cwbhcmdd_MVSDTCP Ready    17106      Running
    cwbhmond_MVSDTCP Ready    18690      Domain Discovered : Mon Aug
    2 17:189

CWBPMMonitor         Ready    19262      Running
cwbsnamapsd          Ready    26422      Ready for client requests
cwbtrapd             Ready    15548      Running
CWBMsgLogServer      Ready    40696      Running
AppnPollerServer     Ready    21386      Connection opened with
cwbsnamapsd

cwbdlswpollerd       Ready    29058      Running
cwbhci_server_MVSDLU62 Initial
cwbhcmd_server_MVSDLU62 Initial
CWBDBAdapter         Ready    33598      Running
cwbmonitord          Initial
```

Step 3 The installation program starts the following applications:

- The Process Manager client, which lets you monitor, start, and stop CiscoWorks Blue processes

- The Message Logger client, which lets you view CiscoWorks Blue messages
- The Administration application, which lets you discover network devices and specify DLSw key devices

Note The Administration application, the Process Manager, and Message Logger clients require X Window System support. If you install the product from a remote workstation, you need an X Window System server and you must export your display to that server to use these applications.

Now that all the servers and processes are running, go to the "Finishing Installation" section on page 3-21 to finish the installation.

Finishing Installation

After the installation process is complete and the CiscoWorks Blue programs are started, you can create a seed file, discover the network routers, and specify DLSw key routers by using the following procedures;

- Creating a Seed File with DLSw Key Routers, page 3-21
- Discovering the Routers, page 3-22
- Running the Verification Program, page 3-22

Creating a Seed File with DLSw Key Routers

This step is optional. A seed file is a file that contains a list of router names or addresses. You can list the routers in either of two formats:

router [*ReadCommunityString*] [**key**]

or

router:[*ReadCommunityString*]:[**key**]

Where:

key indicates that this is a DLSw key device. This option does not apply to APPN/SNASw, RSRB, or TN3270 devices. If you omit the word **key**, the router is not considered a DLSw key device.

For more information on using key devices, see the "Using Key Devices" section on page 2-14.

For information about creating a seed file, see the "Discovering the Network" section on page 7-8 and review creating a seed file in the subsections for each protocol (DLSw, RSRB, TN3270, and APPN/SNASw).

Discovering the Routers

You can discover the network devices using the CiscoWorks Blue Administration application, as described in Chapter 7, "Using the Administration Application."

Now that all the servers and processes are running, and you have created a seed file and discovered the routers in the network, go to Chapter 4, "Monitoring and Controlling CiscoWorks Blue Applications" to learn how to control the applications.

Running the Verification Program

After you finish installing the CiscoWorks Blue products, configuring the products, and discovering routers for the database, use the verification program to ensure that all went successfully. Click **Verify** on the Administration window or enter the commands shown below:

cd /opt/CSCOcb/bin

./cwb verify

The verification program performs the following tasks:

- Summarizes the applications you configured
- Checks your configuration files

- Scans the CiscoWorks Blue database
- Displays a verification report:

```
=============================================================================
                          CiscoWorks Blue Verification
                           Wed Jan 20 14:56:26 1999
                                   nchand-u5
=============================================================================
-----------------------------------------------------------------------------
Process Summary
-----------------------------------------------------------------------------

     Name       Configured      Ready
    ------     ------------    -------
     APPN/SNASw    Yes           Yes
     Base          Yes           Yes
     DLSw          Yes           Yes
     RSRB          Yes           Yes
     TN3270        Yes           Yes
     SNA           Yes           Yes

-----------------------------------------------------------------------------
Database Summary
-----------------------------------------------------------------------------
Total number of devices: 13
    APPN/SNASw:     3
    DLSw:           8
    RSRB:           3
    TN3270:         2

DLSw Key Devices:  6
Physical Units:    7
Logical Units:     7
-----------------------------------------------------------------------------
Action Summary
-----------------------------------------------------------------------------
```

The last section of the report suggests changes you might make to improve the CiscoWorks Blue installation.

- You must fix all errors before you can proceed.
- You can evaluate warnings and take action depending on your needs.
- You can suppress warning messages by setting the *ShowWarnings* parameter in the */opt/CSCOcb/etc/cwbinit* file to **No**.

Configuring the Host Connection

This section describes how to configure the connection between the Maps and SNA View workstation component and the mainframe component. You should configure the host connection *before* you install and configure the workstation.

This section includes the following subsections:

Creating and Deleting a Domain

To create a new domain or delete an existing domain, use the **cwb config** command.

Note Do not copy domain files nor edit them to create new domains. Do not delete domain files to delete existing domains.

Configuring Domain-Specific Parameters

This section describes how to configure domain-specific parameters for an SNA domain. For each SNA domain that you configure, the configuration program creates a file named */etc/svopen_config_DOMAINNAME*, such as */etc/svopen_config_TEXAS* using the domain name and protocol (TCP or LU 6.2)

to create a set of default values in the configuration file. You can edit this file directly, if necessary, to change the values. The following is a sample configuration file:

```
SVMF_AGENT_ADDR rtpmvsd
SVMF_CONNECT TCP
INCLUDE_LUS yes
SVCMD_TIMEOUT 30
SV_KEEPALIVE 30
SV_DISCOVER_DISPLAY TOGGLE
SV_DISCOVER_INTERVAL 10
SV_EVENT_GEN YES
SVPATH /opt/CSCOcb/snahost
SVWORK_AREA /opt/CSCOcb/snahost/tmp
SVCMDS_AGENT_PORT 6100
SVHCI_STATUS_PORT 6101
SVACK_AGENT_PORT 6102
SVHCI_CMD_PORT 6103
SVMF_HCI_AGENT_PORT 6104
SVMF_CMDS_AGENT_PORT 6105
SV_RECONNECT yes
```

Table 3-1 lists the parameters you must set in the configuration file. Table 3-2 lists additional parameters that you might choose to customize. Table 3-3 lists additional parameters whose defaults you might choose to accept.

See the detailed descriptions of all parameters in the sections that follow the tables.

Table 3-1 Required Configuration Parameters

Parameter	Default Value	Description and Valid Values
SVMF_AGENT_ADDR	mvs_host_name.name.com	Host name or IP address of the mainframe on which the mainframe component is installed.
SVMF_CONNECT	TCP	LU62 or TCP. Set to LU62 if you use an LU 6.2 connection.

Table 3-2 Configuration Parameters You Might Want to Customize

Parameter	Default Value	Description and Valid Values
INCLUDE_LUS	YES	YES—Indicates to include LUs in the database. NO—Indicates to exclude LUs from the database.
SVCMD_TIMEOUT	30	1 to 1800 seconds.
SV_INCLUDE_SRB	YES	YES—Calculates PU-SRB dependencies during host discovery. NO—Does not calculate PU-SRB dependencies during host discovery.
SV_KEEPALIVE	30	1 to 1800 seconds.
SV_DISCOVER_DISPLAY	PERCENT	PERCENT.
SV_DISCOVER_INTERVAL	100	1 to 65535 PUs.
SV_EVENT_GEN	YES	YES—Generates an event notification message. NO—Does not generate an event notification message.
SV_LU62CMD_TP	NSPOPNCS	Any valid APPC TP name.
SV_LU62MSG_TP	NSPOPNMS	Any valid APPC TP name.
SV_RECONNECT	YES	YES—If the TCP connection to the mainframe fails, automatically try to reconnect. NO—If the TCP connection to the mainframe fails, do not automatically try to reconnect.

Table 3-3 Configuration Parameters You Might Want to Accept

Parameter	Default Value	Description and Valid Values
SVPATH	/opt/CSCOcb/snahost	Home directory.
SVWORK_AREA	/opt/CSCOcb/snahost	Any valid directory.

Table 3-3 Configuration Parameters You Might Want to Accept (continued)

Parameter	Default Value	Description and Valid Values
SVCMDS_AGENT_PORT	6100	Any unused port value.
SVHCI_STATUS_PORT	6101	Any unused port value.
SVACK_AGENT_PORT	6102	Any unused port value.
SVHCI_CMD_PORT	6103	Any unused port value.
SVMF_HCI_AGENT_PORT	6104	Any unused port value. Must match ports defined in mainframe PARM member.
SVMF_CMDS_AGENT_PORT	6105	Any unused port value. Must match ports defined in mainframe PARM member.

Configuration Parameter Descriptions

The following sections describe each parameter in detail.

- Required Parameters, page 3-27
- Parameters You Might Want to Customize, page 3-28
- Parameters You Might Want to Accept, page 3-31

Required Parameters

Set the following parameters, or accept the default values, for each domain:

- SVMF_AGENT_ADDR (mainframe agent address parameter)—The host name or IP address of the mainframe where the mainframe component is installed. The value is used (and required) only when the SVMF_CONNECT value is **TCP**. There is no default value for this parameter.
- SVMF_CONNECT (mainframe connectivity parameter)—Specifies the method of connectivity to the mainframe. Ensure that this parameter is set correctly:
  - TCP specifies that the workstation is connected to the mainframe using TCP/IP.
  - LU62 specifies that the workstation is connected to the mainframe using LU 6.2.

Parameters You Might Want to Customize

These parameters have preset default values that suit most users. Review the default setting for each parameter and decide whether it meets your requirements. You might want to change some of these parameter values.

- INCLUDE_LUS (include logical units parameter)—Specifies whether to add LUs to the network management database if they are sent from the mainframe. (The Maps and SNA View mainframe installer can use the LU_CONTROL parameter card to specify how LUs are handled.) If your SNA network contains a large number of LUs, you might choose not to monitor them, to conserve workstation resources.
  - YES means the application adds LUs and monitors their status if they are sent from the mainframe.
  - NO means the application does not add LUs.
- SVCMD_TIMEOUT (command time out parameter)—Specifies the number of seconds to wait for a command response from the mainframe before timing out. The default value is 30 seconds.
- SV_INCLUDE_SRB—Determines if a host PU with rif data is associated with the discovered routers.
  - YES means the application calculates the PU-SRB dependencies during host discovery.
  - NO means the application does not perform the calculations.
- SV_KEEPALIVE (Host Connection Interface connection keepalive parameter)—Specifies the number of seconds to wait for each of the following events to occur:
  - For TCP/IP communications, SV_KEEPALIVE controls how long the workstation waits without receiving anything from the mainframe before it sends a ping.
  - For TCP/IP and LU6.2 communications, SV_KEEPALIVE controls how long the Host Connection Interface, Host Command Server, and Status Monitor wait to connect to each other before they determine there is a communications problem.

- SV_DISCOVER_DISPLAY (discovery status message parameter)—Specifies how the Process Manager client displays the discovery status message. The default value is PERCENT.
  - PERCENT—The discovery message window displays the percentage complete.
- SV_DISCOVER_INTERVAL (PU discovery update parameter)—Specifies the number of PUs (1 - 65535) that can be discovered before the Process Manager client application is notified of the discovered PUs. The default is 100 PUs.
- SV_EVENT_GEN (event generation parameter)—Specifies whether the SNA host component generates an event notification message when a VTAM IDBLK/INUM value in the database for one PU is found for a different PU. All event notification messages are described in Chapter 8, “Starting the User Applications.” This condition might mean that more than one end station is trying to use the same PU.
  - YES means the SNA host component generates an event notification message.
  - NO means the SNA host component does not generate an event notification message.
- SV_LU62CMD_TP *tpname*—This parameter card is optional and is required only when a workstation requires multiple host connections using LU6.2. This card allows unique APPC transaction program (TP) names to be specified for each host connection. *tpname* is the APPC TP name configured for the host connection command program. The default name is NSPOPNCS if this card is not defined.
- SV_LU62MSG_TP *tpname*— This parameter card is optional and is required only when a workstation requires multiple host connections using LU6.2. This card allows unique APPC TP names to be specified for each host connection. *tpname* is the APPC TP name configured for the host connection message program. The default name is NSPOPNMS if this card is not defined.
- SV_RECONNECT— For TCP connections only, this parameter determines whether the workstation will automatically try to reconnect if the connection fails. Since a reconnect will restart PU discovery at the mainframe, you might want to manually control this function to avoid high CPU utilization during critical business hours.

– YES means that the application will automatically try to reconnect to the mainframe. This was previously the hardcoded behavior of the product.

– No means that the host connection processes (csbhcid, cwbhmond, and cwbhcmd) will be stopped and will not restart automatically. With this function, host resources will no longer be updated until you manually restart the csbhcid process for this domain.

  You must also alter the /opt/CSCOcb/etc/CWBlue.conf file by changing the cwbhcid process for the proper domain from R “automatically restart” to Y “start automatically (but no restart)”.

  For example, if your domain in”MVSD”, change the following line:

```
cwbhcid_MVSD R CWBMsgLogServer,CWBDBAdapter
/opt/CSCOcb/etc/runprocess cwbhcid_MVSD,MVSD 30

to

cwbhcid_MVSD YCWBMsgLogServer,CWBDBAdapter
/opt/CSCOcb/etc/runprocess cwbhcid_MVSD,MVSD 30
```

See the “Configuring Process Manager Windows” section on page 5-15 for more information on updating the CWBlue.conf file.

Parameters You Might Want to Accept

These parameters have preset default values that suit most users. Review the default setting for each parameter and decide whether it meets your requirements. Depending on how your workstation is configured, you might want to change some of these parameter values.

- *SVPATH* (path parameter)—The home directory of the SNA host component software, which is usually */opt/CSCOcb/snahost*.
- *SVWORK_AREA* (work area directory parameter)—Specifies where the SNA host component places temporary work files. The default is */opt/CSCOcb/snahost/tmp*, but you can change it to meet your site's requirements.
- Port Values:

Port	Default Port Setting
SVCMDS_AGENT_PORT	6100
SVHCI_STATUS_PORT	6101
SVACK_AGENT_PORT	6102
SVHCI_CMD_PORT	6103
SVMF_HCI_AGENT_PORT	6104
SVMF_CMDS_AGENT_PORT	6105

You can change the port values that the SNA host component specifies as default values if any of these ports are already in use at your site. We recommend that the port values be greater than 6000 and not exceed 9999.

When you are managing more than one domain, the Maps and SNA View installation program automatically increments the port values for each specified domain by 20. For example, if a port number in domain ABC is 6100, the SNA host component automatically sets the value for the same configuration parameter in domain DEF to 6120. If the port numbers are already in use, modify them to fit your site's requirements.

Configuring LU 6.2 Connectivity to the Mainframe

This section explains how to configure LU 6.2 connectivity between the SNA host workstation component and the mainframe.

This section includes the following subsections:

Preparing to Configure the SNA Host Component for Maps and SNA View

Before starting the steps to allow the SNA host component on the workstation to communicate with the mainframe, you must first do all the necessary configuration to allow an LU 6.2 session to flow from the workstation to the mainframe. You might need to make changes to both VTAM and the workstation application that supports LU 6.2 sessions. The following workstation LU 6.2 programs are supported:

- HP-UX SNAplus2 (including SNAplus2 Link and SNAplus2 API)
- IBM eNetwork Communications Server for AIX, Version 5.0 or later
- Data Connection SNAP-IX V6.0.6 or later for SPARC Solaris (For more information, see http://www.dataconnection.com)

If the workstation is not directly connected to the mainframe running the SNA host component, but the session instead passes through one or more VTAMs before reaching the destination VTAM, then the correct configuration might require changes to all VTAMs (and possibly NCPs in the path).

Note It is not the intent of this document to identify all the steps necessary to set up the network. See the relevant IBM VTAM and NCP publications for more setup information.

If this LU 6.2 configuration has not yet been done, the installation should be delayed until the LU 6.2 configuration is complete. One way to determine whether there is LU 6.2 connectivity between the workstation and the mainframe is to issue the VTAM command **D NET,APING,ID=***NETID.RESOURCE*. The *NETID.RESOURCE* should be the fully qualified name of the SNA workstation. Until this command returns a positive response, the mainframe will be unable to connect to the workstation.

After the initial LU 6.2 configuration is complete, you can use the procedures in the following sections to complete the configuration for the SNA host component.

Configuring LU 6.2 Connectivity for the eNetwork Communications Server on AIX

If the AIX workstation is connected to the mainframe using SNA LU 6.2, use this procedure to configure the LU 6.2 operating environment. This procedure creates the *sna_tps* file for TP profiles for the command server and the message server and a logmode named PARALLEL.

To configure AIX, create a file named *sna_tps*, and then configure PARALLEL mode processing.

Creating the sna_tps File on AIX

To configure the LU 6.2 transaction programs (TPs) that the SNA host component uses to communicate between an AIX workstation and a mainframe, create the configuration file */etc/sna/sna_tps*, as described in the IBM eNetwork Communication Server for AIX publications. Use the *sna_tps* file to define two TPs named NSPOPNMS and NSPOPNCS. The following example shows a *sna_tps* file:

```
[NSPOPNCS]
LUALIAS = ""
DESCRIPTION = ""
USERID = root
GROUP = system
TIMEOUT = 30
TYPE = NON-QUEUED
STYLE = EXTENDED
PATH = /opt/CSCOcb/bin/cwbstarttp
ARGUMENTS = cwbhcmd_server MYDOMAIN

[NSPOPNMS]
LUALIAS = ""
DESCRIPTION = ""
```

```
USERID = root
GROUP = system
TIMEOUT = 30
TYPE = NON-QUEUED
STYLE = EXTENDED
PATH = /opt/CSCOcb/bin/cwbstarttp
ARGUMENTS = cwbhci_server MYDOMAIN
```

This sample *sna_tps* file defines two TPs:

- NSPOPNCS is for the command server.
- NSPOPNMS is for the message server.

In the file, each TP name is enclosed in brackets, as shown below:

```
[NSPOPNCS]
[NSPOPNMS]
```

For each TP, code the following entries:

- USERID—Specifies the username under which the SNA host component launches the two TPs. This username must be **root**.
- GROUP—Specifies the group for these TP programs (code system, as shown in the sample).
- TIMEOUT—Specifies the timeout period (code **30**, as shown in the sample).
- TYPE—Specifies the type **NON-QUEUED** as shown in the sample.
- STYLE—Specifies the style **EXTENDED** as shown in the sample.

Note When the new eNetwork Communications Server protocol stack is used, you must set the STYLE to **EXTENDED**.

- PATH—Specifies the path to the executable file that handles the transaction programs. Code **/opt/CSCOcb/bin/cwbstarttp**, as shown in the sample.
- ARGUMENTS—Specifies the name of the TP executable file and the name of the SNA domain. Replace MYDOMAIN in the sample file with the name of your SNA domain (use uppercase characters).

Configuring PARALLEL Mode on AIX

After you create the */etc/sna/sna_tps* file, create a new LU 6.2 session profile named PARALLEL as described in the eNetwork Communication Server for AIX publications. Use the **xsnaadmin** command to configure an LU 6.2 PARALLEL logmode. The **xsnaadmin** command can often be found in the */usr/lpp/X11/bin* directory.

Step 1 At the command prompt, enter the **xsnaadmin** command, as shown below.

```
% xsnaadmin
```

The xsnaadmin window is displayed.

Note Ensure that your DISPLAY environment variable is correctly set. You might also have to set the LANG environment variable to your language.

Step 2 In the xsnaadmin window, select **Services > APPC > Modes**.

Step 3 If the PARALLEL mode is not in the list of defined modes, select **Add**. The Add Mode window is displayed.

Step 4 If the PARALLEL mode is already in the list of defined modes, exit the window. If its not in the Add Mode window, enter **PARALLEL** for the Mode Name, and either accept the defaults or customize the values for your operating environment.

If you need to create a PARALLEL log mode, accept the default parameter values:

Field	Default Value
COS name	#CONNECT
Initial session limit	2
Maximum session limit	32767
Min con. winner sessions	1
Auto-activated sessions	0
Receive pacing window (Initial)	4

Configuring LU 6.2 Connectivity for SNAplus2 on HP-UX

This section describes how to configure SNAplus2 for LU 6.2 support on HP-UX. To configure HP-UX SNAplus2, you first create a file named *sna_tps*, and then configure PARALLEL mode processing.

Creating the sna_tps File on HP-UX

To configure the LU 6.2 TPs that the SNA host component uses to communicate between an HP-UX workstation and a mainframe, create the configuration file */etc/opt/sna/sna_tps*, as described in the *SNAplus2 Administration Guide* and *SNAplus2 Installation Guide*. Use the *sna_tps* file to define two TPs named NSPOPNMS and NSPOPNCS. The following example shows a *sna_tps* file:

```
#SNA Host Message Server
["NSPOPNMS"]

PATH          = /opt/CSCOcb/bin/cwbstarttp
ARGUMENTS     = cwbhci_server MYDOMAIN
TYPE          = NON-QUEUED
TIMEOUT       = 30
USERID        = root
GROUP         = sys

#SNA Host Command Server
["NSPOPNCS"]

PATH          = /opt/CSCOcb/bin/cwbstarttp
ARGUMENTS     = cwbhcmd_server MYDOMAIN
TYPE          = NON-QUEUED
TIMEOUT       = 30
USERID        = root
GROUP         = sys
```

This sample *sna_tps* file defines two TPs:

- NSPOPNMS is for the message server.
- NSPOPNCS is for the command server.

  In the file, each TP name is enclosed in quotation marks and then in brackets, as shown below:

  ```
  ["NSPOPNMS"]
  ["NSPOPNCS"]
  ```

For each TP, code the following entries:

- PATH—Specifies the path to the executable file that handles the transaction programs. Code **/opt/CSCOcb/bin/cwbstarttp** as shown in the sample.
- ARGUMENTS—Specifies the name of the TP executable file and the name of the SNA domain. Replace MYDOMAIN in the sample file with the name of your SNA domain (use uppercase characters).
- TYPE—Specifies the type **NON-QUEUED**, as shown in the sample.
- TIMEOUT—Specifies the timeout period (code **30**, as shown in the sample).
- USERID—Specifies the username under which the SNA host component launches the two TPs. This username must be **root**.
- GROUP—Specifies the group for these TP programs (code **sys**, as shown in the sample).

Configuring PARALLEL Mode on HP-UX

After you create the *sna_tps* file, use the **xsnapadmin** command to configure SNAplus2 for PARALLEL processing mode. The **xsnapadmin** command is often found in the */opt/sna/bin/X11* directory.

Step 1 At the command prompt, enter the **xsnapadmin** command, as shown below.

```
% xsnapadmin
```

The xsnapadmin window is displayed.

Note Ensure that your DISPLAY environment variable is correctly set. You might also have to set the LANG environment variable to your language.

Step 2 In the xsnapadmin window, select **Services > APPC > Modes**.

Step 3 If the PARALLEL mode is not in the list of defined modes, select **Add**. The Add Mode window is displayed.

Step 4 If the PARALLEL mode is already in the list of defined modes, exit the window. If its not in the Add Mode window, enter **PARALLEL** for the Mode Name, and either accept the defaults or customize the values for your operating environment.

If you need to create a PARALLEL log mode, accept the default parameter values:

Field	Default Value
Receive pacing window	4
Initial session limit	2
Max session limit	32767
Min con. winner sessions	1
Auto-activated sessions	0

Configuring LU 6.2 Connectivity for SNAP-IX on Solaris

This section describes how to configure SNAP-IX for LU 6.2 support on Solaris. To configure SNAP-IX, you first create the file *sna_tps*, and then configure PARALLEL mode processing.

Creating the sna_tps File on Solaris

To configure the LU 6.2 TPs that the SNA host component uses to communicate between a Solaris workstation and a mainframe, create a configuration file named */etc/opt/sna/sna_tps* as described in the SNAP-IX publications. Use the *sna_tps* file to define two TPs named NSPOPNCS and NSPOPNMS.

The following example shows a *sna_tps* file:

```
[NSPOPNCS]
LUALIAS = ""
DESCRIPTION = ""
USERID = root
GROUP = other
TIMEOUT = 30
TYPE = NON-QUEUED
PATH = /opt/CSCOcb/bin/cwbstarttp
ARGUMENTS = cwbhcmd_server MYDOMAIN
[NSPOPNMS]
LUALIAS = ""
DESCRIPTION = ""
USERID = root
GROUP = other
```

```
TIMEOUT = 30
TYPE = NON-QUEUED
PATH = /opt/CSCOcb/bin/cwbstarttp
ARGUMENTS = cwbhci_server MYDOMAIN
```

This sample *sna_tps* file defines two TPs:

- NSPOPNCS is for the command server.
- NSPOPNMS is for the message server.

  In the file, each TP name is enclosed in brackets, as shown below:

  ```
  [NSPOPNCS]
  [NSPOPNMS]
  ```

For each TP, code the following entries:

- PATH—Specifies the path to the executable file that handles the transaction programs. Code **/opt/CSCOcb/bin/cwbstarttp** as shown in the sample.
- ARGUMENTS—Specifies the name of the TP executable file and the name of the SNA domain. Replace MYDOMAIN in the sample file with the name of your SNA domain (use uppercase characters).
- TYPE—Specifies the type **NON-QUEUED**, as shown in the sample.
- TIMEOUT—Specifies the timeout period (code **30**, as shown in the sample).
- USERID—Specifies the username under which the SNA host component launches the two TPs. This username must be **root**.
- GROUP—Specifies the group for these TPs (code **other**, as shown in the sample).

Configuring PARALLEL Mode on Solaris

After you create the */etc/opt/sna/sna_tps* file, create a new LU 6.2 session profile named PARALLEL, as described in the SNAP-IX publications. Use the **xsnaadmin** command to configure an LU 6.2 PARALLEL logmode. The **xsnaadmin** command can often be found in the */opt/sna/bin/X11* directory.

Step 1 At the command prompt, enter the **xsnaadmin** command, as shown below.

```
% xsnaadmin
```

The xsnaadmin window is displayed.

Note Ensure that your DISPLAY environment variable is correctly set. You might also have to set the LANG environment variable to your language.

Step 2 In the xsnaadmin window, select **Services** > **APPC** > **Modes**.

Step 3 If the PARALLEL mode is not in the list of defined modes, select **Add**. The Add Mode window is displayed.

Step 4 If the PARALLEL mode is already in the list of defined modes, exit the window. If its not in the Add Mode window, enter **PARALLEL** for the Mode Name, and either accept the defaults or customize the values for your operating environment.

If you need to create a PARALLEL log mode, accept the default parameter values:

Field	Default Value
Initial session limit	2
Maximum session limit	32767
Min con. winner sessions	1
Auto-activated sessions	0
Receive pacing window (Initial)	4

Configuring LU6.2 Connectivity to Multiple Hosts

This section allows you to define a single workstation to communicate with multiple mainframes using LU6.2. This section describes the configuration requirements for having a single workstation communicate with multiple hosts using LU6.2:

- There must be unique pair of APPC TP names defined on the workstation for each host connection. The default TP names are NSPOPNMS and NSPOPNCS. Use the appropriate procedure in the "Configuring LU 6.2 Connectivity to the Mainframe" section on page 3-32 to configure APPC TP names and select unique names for each connection.

For example, to have the workstation communicate to both MVS1 and MVS2, configure two sets of APPC TP programs. The pair of TP names for host connection MVS1 could be NSPM1 and NSPC1, while the host connection MVS2 could be NSPM2 and NSPC2.

- In the host connection configuration files, you must indicate which APPC TP names are configured using the SV_LU62CMD_TP and SV_LU62MSG_TP cards.

  For example, for host connection MVS1, the /etc/svopen_config_MVS1 configuration file should specify the following entries:

  – SV_LU62MSG_TP NSPM1

  – SV_LU62CMD_TP NSPC1

  Also, for host connection MVS2, the /etc/svopen_config_MVS2 configuration file should specify the following entries:

  – SV_LU62MSG_TP NSPM2

  – SV_LU62CMD_TP NSPC2

- At each host, ensure the SERVER card definitions in the NSPPARM configuration file match the TP names selected for the host connection.

  For example, at host MVS1 a SERVER card must be configured to indicate TP names of NSPM1 and NSPC1. At host MVS2 a SERVER card must be configured to indicate TP names of NSPM2 and NSPC2.

Configuring TCP/IP Connectivity to the Mainframe

This section explains how to configure TCP/IP connectivity between the workstation and the mainframe. It includes the following subsections:

Configuring TCP/IP Port Parameters

If you configure TCP/IP connectivity from the workstation to the mainframe, you must match the SVMF_HCI_AGENT_PORT and SVMF_CMDS_AGENT_PORT parameters of the domain to the TCP Parameter Cards used in the mainframe. (TCP Parameter Cards are documented in the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide*.) For example, the workstation parameters for domain "NORTH" should be set as follows in */etc/svopen_config_NORTH*:

```
SVMF_HCI_AGENT_PORT 6104
SVMF_CMDS_AGENT_PORT 6105
```

The host configuration file should have a TCP card containing the following:

```
TCP 6104 6105
```

Sending Nonencrypted Data

The data that is transferred between the mainframe and workstation component is not encrypted. This data transfer is secure if the data is transferred over a private intranet. If the workstation-to-host connection traverses the Internet, or if additional security is desired over the intranet, you can use the "Network Data Encryption with Router Authentication" feature provided with Cisco routers to encrypt the data that flows between the router nearest to the workstation and the router nearest to the host.

For more information on this topic, see the Cisco IOS software *Security Configuration Guide*.

Configuring Connectivity to Multiple Domains

If you configure TCP/IP connectivity from the same workstation to multiple mainframe domains, each set of SVMF_HCI_AGENT_PORT and SVMF_CMDS_AGENT_PORT parameters for each domain must have corresponding TCP parameter cards in the mainframe. (TCP Parameter Cards are documented in the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide*.)

To configure connectivity from the same workstation to multiple mainframe domains, use the following procedure:

For example, the workstation parameters for domain NORTH should be set as follows in */etc/svopen_config_NORTH*:

```
SVMF_HCI_AGENT_PORT 6104
SVMF_CMDS_AGENT_PORT 6105
```

The workstation parameters for domain SOUTH should be set as follows in */etc/svopen_config_SOUTH*:

```
SVMF_HCI_AGENT_PORT 6114
SVMF_CMDS_AGENT_PORT 6115
```

The host configuration file for the SNA Host component at each domain's mainframe should have a TCP cards that contain the following lines:

- For domain NORTH:

  ```
  TCP 6104 6105
  ```

- For domain SOUTH:

  ```
  TCP 6114 6115
  ```

Applying Licenses after Installation

If you choose not to apply your CiscoWorks Blue license information during installation, or if you later obtain a new license for Maps or SNA View, you can apply a license after installation as described in this section.

You can get one of two licenses for the CiscoWorks Blue applications. You can get a license to run the Maps applications and a license to use the SNA View web pages. The license that you obtain determines which CiscoWorks Blue applications you can run. If you license both Maps and SNA View, you can use all the applications:

- The SNA View license enables the SNA View icon on the CiscoWorks Blue web page and TN3270 discovery.
- The Maps license enables the DLSw, RSRB, and APPN/SNASw icons on the CiscoWorks Blue web page, and makes the DLSw, RSRB, and APPN/SNASw Motif applications operational.

- Either license enables the Process Manager, Message Log Viewer, and Administration program, as well as discovery of DLSw, RSRB, and APPN/SNASw devices.

After installation, use the **cwbupgrade.sh** command to apply the Maps and SNA View license keys. To enter a license key, use the following procedure:

Step 1 Start the */opt/CSCOcb/install/cwbupgrade.sh* program:

/opt/CSCOcb/installcwbupgrade.sh

Step 2 When you see the following prompt, enter **y** to enter a license key:

```
Do you want to enter CiscoWorks Blue Maps license key [yes|no]? Y
```

Step 3 When you see the following prompt, enter the Maps license key:

```
Enter the CiscoWorks Blue Maps license key (example 123456789012) or
press enter if not licensed for CiscoWorks Blue Maps: 123456789012
```

Step 4 When you see the following prompt, enter the SNA View license key:

```
Enter the CiscoWorks Blue SNA View license key (example 123456789012)
or press enter if not licensed for CiscoWorks Blue SNA View:
123456789012
```

Step 5 If you applied a temporary license key for an evaluation copy of Maps or SNA View, or a license key that is invalid, you might see one of the following messages:

```
INFO:Your current CiscoWorks Blue Maps license expires on mm/dd/yyy.
Do you want to enter CiscoWorks Blue Maps license key[yes|no]? [Y]

INFO:Your current CiscoWorks Blue SNA View license expires on
mm/dd/yyy.
Do you want to enter CiscoWorks Blue SNA View license key[yes|no]? [Y]

INFO:Your current CiscoWorks Blue Maps license key is not valid.
Do you want to enter CiscoWorks Blue Maps license key[yes|no]? [Y]

INFO:Your current CiscoWorks Blue SNA View license key is not valid.
Do you want to enter CiscoWorks Blue SNA View license key[yes|no]? [Y]

Press Enter if you now want to apply a valid, permanent license key
for Maps or SNA View.
```

Step 6 If Maps or SNA View is now running, press **Enter** when you see the following prompt:

```
INFO: CiscoWorks Blue Servers are currently running. You must restart
all CiscoWorks Blue processes to make these changes effective.
Do you want to restart CiscoWorks Blue processes [yes|no]? [Y]
```

Configuring CiscoWorks Blue after Installation

You can configure the CiscoWorks Blue applications after installation using the **cwb config** command.

Step 1 Enter the following commands:

cd /opt/CSCOcb/bin

./cwb config

Step 2 Make your responses to the configuration prompts as described in the "Configuring CiscoWorks Blue" section on page 3-11.

Deinstalling CiscoWorks Blue

If you have a previous version of CiscoWorks Blue installed, you must deinstall it before installing Release 3.0.1. If you have errors during installation of 3.0.1, you might also need to run uninstall before trying to install it again.

This section describes how to deinstall CiscoWorks Blue Maps and SNA View, and contains the following sections:

- Deinstalling CiscoWorks Blue From a Previous Release, page 3-46, describes how to deinstall a previous release of CiscoWorks Blue software before you reinstall the product.

Deinstalling CiscoWorks Blue From a Previous Release

Note When you deinstall the previous release and then install Release 3.0.1, the following configuration files are saved in the */var/tmp/cwb.save* directory: *cwbinit*, *runprocess*, *CWBlue.conf*, *Services.conf*, and *SeedFile*.

Step 1 Log in as the root user. For details, see the "Becoming the Root User" section on page 2-13.

Step 2 If you are deinstalling Release 3.x, use the following command from the CD to preserve the license keys:

/cdrom/uninstall.sh

If you are deinstalling Release 2.x, start the interactive deinstallation script by entering the following commands:

cd /opt/CSCOcb/install

./uninstall.sh

Note To deinstall Release 2.x, do not run uninstall from the CD because the license keys for Release 2.x will not work with Release 3.0.1.

After you issue the **uninstall** command, the deinstallation script lists the packages that are installed:

- CSCOcwbC is a common package that supports Maps and SNA View.
- CSCOcwb*XX* is the Maps and SNA View package that supports an NMS. The *XX* identifies the NMS. (For example, package CSCOcwbOV supports HP OpenView.)
- CSCOjre102 and CSCOjre110 provide Java Runtime Environment support (for HP workstations only).

Step 3 In reply to the following prompt, enter **Y** or press **Enter** to deinstall the packages.

```
Delete all Cisco Products CiscoWorks Blue packages listed above? [yes]
```

The deinstall program removes the CiscoWorks Blue products from the system.

Note If the program fails to completely uninstall all CiscoWorks Blue files and directories from the */opt/CSCOcb* file structure, run **uninstall.sh** again.

Modifying Color Schemes for the Maps Motif Applications

After installation, you can modify the color scheme of the Maps Motif applications by copying the *Color.schemename* file in the */opt/CSCOcb/Xdefaults* directory to the file named */opt/CSCOcb/Xdefaults/Color*.

Here is an example that shows how to copy the *Color.Rembrandt* file as *Color*:

cd /opt/CSCOcb/Xdefaults

cp Color.Rembrandt Color

Running the Maps Applications with a Sample User

After installation is complete, the installation process creates a sample user with the username cwblue. The username cwblue is created without a password. To start a Maps application from the command line, you can do one of the following:

- Create a password for the cwblue username.
- Log in as the root user and use the switch username command to become user cwblue:

  # su - cwblue

- Then you can start one of the Maps Motif applications using the **cwb start** command.

Note You must be the root user to start the server processes.

CiscoWorks Blue Maps Environment Variables

This section lists the environment variables that are set automatically by the CiscoWorks Blue Maps script (**runprocess**). Table 3-4 lists the environment variables, used by each application (for technical reference only).

Table 3-4 Maps and SNA View Environment Variables

Variable	Use and Default Value
CSCO_TVSPATH	CiscoWorks Blue Maps bitmap directory; the default is *$CWBROOT/Xbm*.
CVIEWROOT	CiscoView installation directory.
CWB-ALIVE-TIMEOUT	Discover-in-progress timeout to detect abnormal termination of discovery process.
CWB-CONNECT-TIMEOUT	Time required for discovery process to initially contact progress indicator window.
CWB_MAPNOTEXIST	Tells Maps application not to read the layout from a saved map file, which forces the application to create a new layout; by default it is not set. This variable is for use when you are instructed to create a new layout by the Cisco TAC to solve a layout problem.
CWBCSROOT	CiscoWorks Blue common code directory.
CWBROOT	CiscoWorks Blue Maps installation directory; set to the directory you specify during installation, usually */opt/CSCOcb.*
CWB_DEFAULT_LAYOUT	Sets the default layout of graphical maps; values can be C (circular), H (hierarchical), or S (symmetrical). The default value is H.

Table 3-4 Maps and SNA View Environment Variables (continued)

Variable	Use and Default Value
CWB_MIBFILE	Specifies the name of the MIB file; defaults to *$CWBROOT/etc/mib.txt*.
CWB_PROCESS_ REFRESH	Specifies the refresh interval, in seconds, for the Update Process window.
CWB_SERVER	Identifies the workstation on which the daemons run. The default is *hostname*.
CWB_UPDATE_ INTERVAL	Defines an interval to control map refresh requests. During this period, map changes are recorded but not displayed. When the interval expires, the map is refreshed. The default value is 10 seconds.
CWB_UPDATE_ SERVER	Identifies the workstation on which the cwbmonitord daemon runs. The default is $CWB_SERVER.
DBNAME	Name of the CiscoWorks Blue database, such as *SNA*.
DSQUERY	Name of the Sybase database server, such as CW_SYBASE.
HHHOME	HyperHelp installation directory for CiscoWorks Blue Maps help. The default is *$CWBROOT/hyperhelp*.
INSTALL_SOL_27	Allows installation on Solaris Version 7 when set to TRUE.
INSTALL_SOL_28	Allows installation on Solaris Version 8 when set to TRUE.
INSTALL_AIX_51	Allows installation on AIX Version 5.1 when set to TRUE.
LD_LIBRARY_ PATH	Set runtime library search path for Solaris.
LIB_PATH	Sets the runtime library search path for AIX.
NETMGTSYS	Indicates whether an NMS is integrated with CiscoWorks Blue. NONMS indicates no NMS is integrated.
NMSROOT	CiscoWorks installation directory.

Table 3-4 Maps and SNA View Environment Variables (continued)

Variable	Use and Default Value
PRINTER	Printer identification. The default is none; if printing maps is desired, set this before starting any Maps application.
SHLIB_PATH	Set runtime library search path for HP-UX.
SQLANY	Directory path to SQLAnywhere, such as */opt/CSCOcwbC/db.*
SVHOME	CiscoWorks Blue the SNA Host component installation directory. The default is *$CWBROOT/snahost*.
SYBASE	Sybase installation directory, such as */opt/CSCOcwbC/db/ctlibs*.
TERM	Specifies xterm terminal.
XAPPLRESDIR	CiscoWorks Blue Maps X resource directory. The default is */opt/CSCOcb/Xdefaults*.

CHAPTER 4

Monitoring and Controlling CiscoWorks Blue Applications

This chapter presents an overview of the procedures necessary to administer the CiscoWorks Blue Maps and SNA View user applications. As administrator, your job entails using the various CiscoWorks Blue administration programs to:

- Start and stop the CiscoWorks Blue daemons and processes
- Control the message log and view the error messages
- Ensure that all the configuration files are correct
- Specify DLSw key devices and discover the network devices (routers) that support the SNA and TCP/IP protocols
- Use the product verification utility to ensure that everything is ready for the users to run the Maps and SNA View Motif and web-based applications
- Use the **cwb** command scripts to perform many administrative tasks
- Start and control the CiscoWorks Blue web server

This chapter includes the following main sections:

Starting Processes and Servers During Installation

At the end of product installation, you are asked whether you want to start the CiscoWorks Blue servers and processes. If you answered **Yes**, the following servers are started:

- Naming server
- Process Manager server

Any processes marked as autostart are started by the Process Manager. You can see which programs have been started by using the **cwb show status** command:

/opt/CSCOcb/bin/cwb show status

The output from this command shows you the status and process ID of all servers and processes. The Last Message column displays the last message sent by the process to the Process Manager.

```
CiscoWorks Blue Naming Server Started.
CiscoWorks Blue Process Manager Started.
Process Manager running with processes:

PROCESS              STATE    PID        Last Message

CWBHTTPAdapter       Ready    45818      Running
CWBOSAMonitor        Ready    25078      Running
cwbhcid_MVSDTCP      Ready    26162      Running
  cwbhcmdd             Ready    17106      Running
  cwbhmond             Ready    18690      Domain Discovered : Mon Aug
2 17:189
CWBPMMonitor         Ready    19262      Running
cwbrsrbpollerd       Ready    27004      Running
cwbsnamapsd          Ready    26422      Ready for client requests
cwbtrapd             Ready    15548      Running
```

```
CWBMsgLogServer      Ready    40696      Running
AppnPollerServer     Ready    21386      Connection opened with
cwbsnamapsd
cwbdlswpollerd       Ready    29058      Running
cwbhci_server_MVSDLU62 Initial
cwbhcmd_server_MVSDLU62 Initial
CWBDBAdapter         Ready    33598      Running
cwbmonitord          Initial
```

Administering CiscoWorks Blue after Installation

This section describes the ongoing administration tasks that you will perform after successful installation of the CiscoWorks Blue products. This section includes the following information:

Applying the CiscoWorks Blue Licenses

To run the CiscoWorks Blue Maps and SNA View applications and their supporting servers and processes, you must obtain and apply the appropriate license information. You obtain licenses from Cisco to run Maps and SNA View and you apply the license information in one of the following two ways:

- During the installation process, you can provide the license keys in answer to the questions asked by the installation script.
- After installation is complete, you can use the **cwbupgrade.sh** command as described in the "Applying Licenses after Installation" section on page 3-43.

Monitoring and Controlling Processes

The Process Manager client lets you view the status of processes and daemons and it lets you start and stop the processes and daemons. You can start the Process Manager client in one of the following ways:

- From the Administration application, as described in Chapter 7, "Using the Administration Application"
- Enter the **cwb start ProcMgrClient** command:

  /opt/CSCOcb/bin/cwb start ProcMgrClient

Use the **cwb show status** command to monitor the status of the CiscoWorks Blue servers and processes:

/opt/CSCOcb/bin/cwb show status

For information about using the Process Manager, see Chapter 5, "Using the Process Manager."

You can also use the **cwb** script to start processes, daemons, user applications, and other administrative programs from the command line, as described in Appendix D, "CiscoWorks Blue Commands and Processes."

Viewing the Message Log

The Message Log client lets you view the messages that are logged by CiscoWorks Blue processes and control the kind of messages that are logged. You can start the Message Log client in one of the following ways:

- From the Administration application, (as described in Chapter 7, "Using the Administration Application")
- Enter the **cwb start MsgLogClient** command:

  /opt/CSCOcb/bin/cwb start MsgLogClient

For information about using the Message Log, see Chapter 6, "Using the Message Log Viewer."

Completing the cwbinit File

The */opt/CSCOcb/etc/cwbinit* file contains default values used by most of the CiscoWorks Blue applications.

Specifying an APPN/SNASw Network Topology Agent

In most cases you will not be able to specify a network topology agent because SNASw as a branch network node does not have the complete APPN topology. Leave this field blank in the APPN motif startup and the /opt/CSCOcb/etc/cwbinit file unless you have an APPN Network Node that supports the APPN-MIB in your network. Even without a network topology agent, the network topology views will be avilable, populated from the information retrieved from the managed SNASw routers.

For more information about specifying a network topology agent, see the "Selecting a Network Topology Agent" section on page 8-19.

Specifying NetView and CiscoWorks 2000 Web Addresses

If you also use Cisco View or CiscoWorks 2000, you must access those software packages at the following URL:

http://<CiscoWorks URL or IP Address>:<CiscoWorks Port>/CSCOnm/servlet/com.cisco.nm.cvw.servlet.CvServlet?csUser=autoLogin&Device=<*device name or IP Address*>

CiscoWorks Blue fully qualifies device domain names to CiscoWorks 2000, including the Cisco View feature, to ensure that the resource is correctly identified in CiscoWorks 2000.

To link from the CiscoWorks Blue web page to web pages for NetView for OS/390 and CiscoWorks 2000, you can set these URLs in *cwbinit*, as described in the "Starting and Stopping the Web Server" section on page 4-11.

Setting DLSw and RSRB Polling Intervals

Use the *cwbinit* file to set polling intervals for DLSw and RSRM devices, as described in the "Starting and Stopping the Web Server" section on page 4-11.

Specifying Values for the cwbsnamapsd Web Daemon

Use the *cwbinit* file to specify values to control the *cwbsnamapsd* web daemon, as described in the "Starting and Stopping the Web Server" section on page 4-11.

Starting Host Discovery

To correlate the SNA PUs with the TCP/IP routers, you must run the SNA host discovery process. If, during installation, you select a TCP connection to the mainframe, then the Process Manager automatically starts the cwbhcid daemon to start a host connection.

To start the daemon in the Process Manager, click **cwbhcid_domain** and click **Start**. If you selected an LU 6.2 connection to the mainframe, you must first configure the LU 6.2 transaction programs as described in the section "Configuring the Host Connection" section on page 3-24. The CiscoWorks Blue mainframe application will actually start the connection to the workstation.

Creating a Seed File

You can use a seed file for discovering routers and for specifying DLSw key routers. A seed file is a file that contains a list of routers to be discovered. You can list the routers in either of two formats:

router [*ReadCommunityString*] [**key**]

or

router:[*ReadCommunityString*]:[**key**]

Where **key** indicates that this is a DLSw key device. If you omit the word key, the router is not considered a DLSw key device.

For information about creating a seed file, see the "Discovering the Network" section on page 7-8 and view the subsections specific for each protocol (DLSw, RSRB, TN3270, and APPN/SNASw).

Specifying DLSw Key Devices

For DLSw applications, whether web-based or Motif applications, you should select several routers as key devices. For information about key devices, see the "Specifying the Status of Aggregated Peers" section on page 7-14.

Select key devices in one of the following ways:

- Before you run the discovery process, you can specify key devices in a seed file using the *key* parameter to designate that router as a key device. For information about the seed file, see the "Discovering the Network with a Seed File" section on page 7-9.
- After you run the discovery process, you can specify key devices using the CiscoWorks Blue Administration application, as described in the "Launching the Process Manager Client" section on page 7-38.
- After you run discovery, from the Motif-based DLSw application, you can specify key devices by selecting **Edit > Key Device(s)** from the menu bar, as described in Chapter 8, "Starting the User Applications." (This option is available only if you have licensed CiscoWorks Blue Maps.)

Discovering the Routers

You discover the TCP/IP-managed devices (routers) in the network to populate the CiscoWorks Blue database. During this time, the discovery process discovers and records every device in the network that supports any of the supported protocols (DLSw, RSRB, APPN/SNASw, or TN3270).

Discover the network devices using the following applications:

- From the CiscoWorks Blue Administration application, as described in Chapter 7, "Using the Administration Application."

Note To see SRB rings in DLSw views, including the SNA dependency views, use RSRB/SRB discovery from the Administration application.

- From the Motif applications, by selecting **Tools > Discover** from one of the Maps Motif applications (DLSw, APPN/SNASw, or RSRB), as described in Chapter 8, "Starting the User Applications." (This option is available only if you have licensed CiscoWorks Blue Maps.)

Discover the network devices in one of the following ways:

- Use the database maintained by a network management system (NMS), such as NetView for AIX, HP OpenView, and SunNet Manager. For more information, see the "Discovering the Network" section on page 7-8 and review the subsection for each protocol (DLSw, RSRB, and APPN/SNASw).
- Use a list of routers that you create in a seed file. For more information, see the "Discovering the Network" section on page 7-8 and review the subsection for each protocol (DLSw, RSRB, and APPN/SNASw).

Note If you discover DLSw devices from a seed file, you should specify key devices in the seed file.

Setting a Password for the cwblue User

During installation, (if CiscoWorks is also installed) user ID cwblue is created for running CiscoWorks Blue applications. The user ID is created without a password, so you may want to create a password for cwblue before you let users log in with it.

Verifying That CiscoWorks Blue Is Ready

Run the product verification program to ensure that all the preceding tasks were done correctly. The verification program checks the contents of the configuration files and the CiscoWorks Blue database for accuracy and completeness and ensures that all the required servers and processes are running so that users can log in to the web page and use the Motif applications.

You can run the verification program from the administration program, as described in Chapter 7, "Using the Administration Application," or by issuing the following command:

/opt/CSCOcb/bin/cwb verify

Using the cwb Command

The **cwb** command performs a variety of related administration tasks, such as starting and stopping servers and processes and displaying status. The **cwb** command is summarized here, but is explained in full, with command line options, in Appendix D, "CiscoWorks Blue Commands and Processes."

- To start and stop specific servers, use one of the following commands:

  cwb {start | stop} [pm | name]

  cwb start servers

- To start and stop processes, use one of the following commands:

  cwb {start | stop} *process_name*

  cwb stop all

See Appendix D, "CiscoWorks Blue Commands and Processes" for information about the processes that you can start and stop. The **cwb stop all** command stops the Process Manager too. Use the **cwb kill all** command only when you cannot stop processes normally.

- To kill all CiscoWorks Blue processes, use the following command:

  cwb kill all

- To start the Administration application, use the following command:

  cwb start admin

- To start the discovery application, use the following command:

  cwb start cwbdiscover [-d [d][r][a][t]]

- To start the DLSw Motif application, use the following command:

  cwb start dlsw

- To start the RSRB Motif application, use the following command:

  cwb start rsrb

- To start the APPN Motif application, use the following command:

  cwb start appn

- To start the Message Log client, use the following command:

  cwb start MsgLogClient

- To start the Process Manager client, use the following command:

  cwb start ProcMgrClient

- To display status and version information, use the following command:

  cwb show {versions | status}

- To create a seed file from the CiscoWorks Blue database, use the following command:

  cwb create seed

- To clear all data from the CiscoWorks Blue database and the *appnfile* file, use the following command:

  cwb clear db

- To run the CiscoWorks Blue configuration program to reconfigure host connection and port usage, use the following command:

  cwb config

- To verify successful installation of CiscoWorks Blue products, use the following command:

  cwb verify

- To collect information for reporting to Cisco TAC, use the following command:

  cwb tac [-o *outputdirectory***]**

- Toperform maintenance or to start the maintenance schedule, use the following command:

  cwb maintenance [start | stop]

Starting and Stopping the Web Server

Before you access the CiscoWorks Blue web page from a web browser, ensure that the web server is running on the workstation on which the CiscoWorks Blue applications are installed. To determine whether a web server is running, enter the following commands:

cd /opt/CSCOcb/bin

./cwb show status

If the CiscoWorks Blue web server is not running, you can start it using the Process Manager.

The CiscoWorks Blue web server starts using the port that was configured during installation and configuration. The order of port selection is as follows:

1. Use port 80.
2. Use port 8080.
3. Ask installer for unused port.

Browse the file */opt/CSCOcwbC/apache/etc/httpd.conf* to find the port being used.

Using the cwbinit File

The *cwbinit* file contains a set of startup options and variables with which the *cwbsnamapsd* application starts.

- The first set of parameters in the *cwbinit* file are used only by the *cwbsnamapsd* application.
- The second set of parameters in the *cwbinit* file are used by both the *cwbsnamapsd* application and the APPN/SNASw application.

If you change the *cwbinit* file while the application is running, you must reset the process to activate the changes to *cwbinit*.

Parameters for cwbsnamapsd Only

The following sample of the *cwbinit* file shows just the values that apply to the *cwbsnamapsd* application:

```
# ********************************************************************
# This section is used by the cwbsnamapsd server process, which
# handles requests from the web interface.

# default socket number for communication with cgi-bin programs
socketCgi-AppServer = 51999

# default number of threads for cwbsnamapsd.
# Valid range of values is 1 to 30.
# Increase the number to allow more concurrent web browser users,
# decrease the number to limit CPU utilization on the server.
socketPoolThread = 10
```

```
# cgi-bin wait time on response from cwbsnamapsd, in seconds.
# This is used to clean up outstanding requests in case of a hang or
# other problems with cwbsnamapsd.
# Increase this value only if time outs occur because of extremely
# slow network (snmp) or database responses.
cgiBinWaitTimeOut = 120

# TME 10 NetView for OS/390 Web Interfaces
#
# This is used to configure the NetView Web Interfaces used by the
# Maps/SNA View.  Each NetView login must contain a name and URL
# separated by a '^' character.
#
# The name is any identifier that you want to associate with the
# NetView login.  The URL is the fully-qualified address of the
# NetView web interface.
#
# You may specify multiple NetView logins, each of which must be
# separated by a ',' character:
# netViewInterfaces = name^url,name^url,name^url
# For example:
# netViewInterfaces = Joe's NetView^www.myhost.com,Bob's
# NetView^www.myhost.com/~bob

netViewInterfaces =

# CiscoWorks 2K Web Interface
# This is used to indicate the URL of the CiscoWorks 2000 Resource
# Manager Essentials
# package:

# ciscoWorksURL = http: //<host name>:<port>

ciscoWorksURL =

# SNA Filter Request Database Limit
#
# Whenever you make a request to the database, the application first
# calculates the amount of data that needs to be processed to service
# the request.  This parameter indicates at what point the request is
# considered too big and should not be processed.
#
# When you submit a request, the 'cgiBinWaitTimeOut' parameter
# controls how long the browser will wait until it times out. If you
# submit a huge request to the database (like 'LU Name=*'), the web
```

```
# server will most likely timeout before the database ever finishes
# processing the request. This parameter is used to filter out those
# requests that will probably never finish before the web browser
# times out. You will get a message on the web interface informing
# you that this limit has been reached, and you should refine your
# search.
#
# You can adjust this parameter to suit your needs. The higher the
# number, the larger the request the database will try to handle.
# Keep in mind, however, that a larger number will cause the database
# to work harder, thereby affecting system performance and blocking
# database access to other users of this application.
#
# In the normal course of operations, the requests to the database
# should not be all that large.  If they are, then the users of the
# product should
# narrow down their requests to the database by specifying more
# precise data in the SNA Filter search screens.

maxRowCount = 5000

# SNA View Sessions and Session Connectivity Field Suppression
#
# The following allow the indicated field name and the related
# contents to be suppressed in the Sessions table and on the Session
# Connectivity display. By default, all fields and their associated
# values are displayed.
# To suppress a field and its contents, uncomment the field entry. You
# may want to do this to reduce the Sessions table width or to block
# sensitive data from being displayed to SNA View users.
#
# To turn on the field name suppression, set the associated variable =
# on. Valid values : on/off. default value : off.

#suppressLUName = on
#suppressPU2Name = on
#suppressFEPName = on
#suppressLogicalLineInfo = on
#suppressPhysicalLineInfo = on
#suppressClientIP = on
#suppressMACSAP = on
#suppressIDBLKNUM = on
#suppressCPName = on
#suppressDLURName = on
#suppressDLUSName = on
#suppressNodeName = on
```

socketCgi-AppServer

Use the **socketCgi-AppServer** value to specify the socket number to use when communicating with cgi-bin web programs. The default socket number is 51999.

socketPoolThread

Use the **socketPoolThread** value to specify the number of threads for *cwbsnamapsd*. The valid range of values is 1 to 30. The default is 10 threads. You can increase the number of threads to allow more concurrent web browser users, and you can decrease the number of threads to limit CPU use on the server.

cgiBinWaitTimeOut

Use the **cgiBinWaitTimeOut** value to specify the cgi-bin wait time on response from *cwbsnamapsd*, in seconds. This value is used to clean up outstanding requests in case of a hang or other problems with *cwbsnamapsd*. Increase this value only if time outs occur because of extremely slow network (snmp) or database responses. The default value is 120 seconds.

netViewInterfaces

Use the **netViewInterfaces** value to configure the NetView web interfaces used by the CiscoWorks Blue web page. Each NetView login must contain a name and URL separated by a "^" character.

- The name is any identifier that you want to associate with the NetView login.
- The URL is the fully-qualified address of the NetView web interface.

You can specify multiple NetView logins, each of which must be separated by a comma (,) in the following format:

```
netViewInterfaces = name^url,name^url,name^url
```

For example, you might enter the following:

```
netViewInterfaces = Joe's NetView^www.myhost.com,Bob's
NetView^www.myhost.com/~bob
```

ciscoWorksURL

Use the **ciscoWorksURL** value to configure a CiscoWorks 2000 web Interface. This value is used to indicate the URL of the CiscoWorks 2000 Resource Manager Essentials package. Use the following format:

```
ciscoWorksURL = http: //host_name[:port]
```

Where:

host_name is the host name of the host running the CiscoWorks 2000 web Interface.

port is the port number on that host, if it is not port 80.

Session Field Suppression

Use the set of "SNA View Sessions and Session Connectivity Field Suppression" variables to do the following:

- Configure the fields that can be suppressed on the SNA View Sessions tables.
- Configure the information that is suppressed in a dependency view.

Initially, the session suppression entries are set as comments so they are not active. Each value lets you suppress one or more related fields. For example, to suppress the display of the IDBLK/IDNUM field, you would uncomment the *suppressIDBLKNUM* line, as shown below:

```
suppressIDBLKNUM = on
```

You can suppress displaying fields, as shown in the following table:

This parameter...	Suppresses these fields...
suppressLUName = on	LU Name
suppressPU2Name = on	PU2 Name
suppressFEPName = on	FEP Names
suppressLogicalLineInfo = on	Logical Line PU field and logical line information in the dependency view
suppressPhysicalLineInfo = on	Physical line information in the dependency view
suppressClientIP = on	Client IP address

This parameter... (continued)	Suppresses these fields...
suppressMACSAP = on	Client MAC/SAP and destination MAC/SAP or MAC1/SAP1 and MAC2/SAP2
suppressIDBLKNUM = on	IDBLK/IDNUM
suppressCPName = on	CPNAME
suppressDLURName = on	DLUR Name
suppressDLUSName = on	DLUS Name
suppressNodeName = on	Node Name

Parameters for cwbsnamapsd and APPN/SNASw

The following sample of the *cwbinit* file shows the values that apply to the *cwbsnamapsd* application and to APPN/SNASw.

```
[cwbsnamapsd and  APPN/SNASw Parameters Begin Here]

# **********************
# ***  APPN/SNASw parameters ***
# **********************
# These parameters are used by both  APPN/SNASw and cwbsnamapsd. If
either
# is already running, they must be stopped and restarted for changes
# to take effect.

# Selection of the network topology agent is done in this order:
# 1) command line parameters, if any;
# 2) parse this config file.
# 3) user will be prompted to run discovery or enter agent information
#
# 3 applies to  appn only. No prompt dialog is given in cwbsnamapsd.

# network topology agent ip address or device name (NOT  appn cpname)
nettopoagentdevname =

# network topology agent read community string
nettopordcommstr =

# network topology agent  appn control point name (NETID.CPNAME
format)
nettopoagentcpname =

# backup network topology agent ip address or device name (NOT  appn
```

```
# cpname)
backupnettopoagentdevname =

# backup network topology agent read community string
backupnettopordcommstr =

# backup network topology agent  appn control point name (NETID.CPNAME
# format)
backupnettopoagentcpname =

# default read community string
rdcommstr = public

# automatic collection of local topology (NONE, NN_ONLY, ALL)
autolocaltopo = ALL

# network topology polling interval, in seconds
nettopopoll = 15

# backup network topology polling interval, in seconds
# (in backup mode only, when primary agent fails, backup uses
nettopopoll)
backupnettopopoll = 600

# local topology polling interval, in seconds
loctopopoll = 600

# control whether  APPN/SNASw polls the DLUR PU table as part of local
# topology polling. To turn off polling for PUs, set appn_pu_polling =
# off
appn_pu_polling = on

# control whether  APPN/SNASw polls the  APPN/SNASw port table as part
of local
# topology polling. To turn off polling for ports, set
# appn_port_polling = off
appn_port_polling = on

# control whether  APPN/SNASw polls the  APPN/SNASw link table as part
of local
# topology polling. To turn off polling for links, set
# appn_link_polling = off
appn_link_polling = on

# This option controls TG event generation.
# To turn off TG event generation, set eventgen_tg = off.
# To generate event for existing TGs when an operational state change
# is detected, set eventgen_tg = on.
```

```
# To generate events for existing TGs when an operational state change
# is detected and for newly created operational (active) TGs,
# set eventgen_tg = all.
# Exception: No events are generated for TGs created on
# the first poll cycle. This avoids a storm of events during
# process startup.
# valid values: on/off/all
eventgen_tg = on

# To turn off dlur session event generation, set eventgen_dlur = off
# valid values : on/off
eventgen_dlur = on

# To turn on port event generation, set eventgen_port = on
# valid values : on/off
eventgen_port = off

# To turn on link event generation, set eventgen_link = on
# valid values : on/off
eventgen_link = off

# This option controls the CWBlue cache deletion of TGs that are no
# longer reported by local topology agents. A Cisco IOS change was
# made to delete inactive dynamic TGs from the router database.
# To delete TGs that are no longer reported by the agent,
# set this parameter to 'off'.
# To keep those TGs in the CWBlue cache, set this parameter to 'on'.

If TG
# events are enabled, this will trigger an event if the TG becomes
# operational again.
# valid values:on/off
keep_deleted_tgs = off
```

Controlling Access to the CiscoWorks Blue Web Page

You can use various methods to control access to the CiscoWorks Blue web page. You can find documentation about Apache HTTP server Version 1.3.26 security features at the following web sites:

- http://www.apacheweek.com/features/userauth
- http://www.apacheweek.com/features/dbmauth

The CiscoWorks Blue web server supports both **htpasswd** and **dbmmanage** methods of user authentication documented in these URLs.

Communicating the Maps and SNA View URL

After you install Maps and SNA View, your Maps and SNA View users can elect to use a web browser to access the applications. These users start their web browsers and type the URL of the CiscoWorks Blue web server:

`http://host_name[:port_number]/`

Where:

host_name is the name of the host on which you installed Maps or SNA View.

port_number is the number of the port used by the web server. If port 80 is used, the port number can be omitted.

For example, if your host name is host.cisco.com, and the port is 8080, users would type:

http://host.cisco.com:8080/

If your host name is host.cisco.com, and the port is 80, users would type:

http://host.cisco.com/

Enabling DNS Lookups for Device Queries

The *doDNSSearch* variable in the *cwbinit* file lets you specify that a domain name server (DNS) lookup will be done for queries to routers during discovery and polling. For example, using DNS lookup, a device that was discovered as *heritage.cisco.com* could also be referred to as *heritage*. You can set this variable so that you can enter a different name that will be resolved by a DNS lookup. This variable is used when you do the following:

- Discover devices with the Maps and SNA View web interface
- Use the Administration program to discover, rediscover, and add devices
- Use the **cwb start cwbdiscover** command
- Use discovery or add devices in the Maps Motif application
- Use the web interface that relies on *cwbsnamapsd* to provide updated information

The following new section of the *cwbinit* file provides the *doDNSSearch* variable:

```
# ****************************************************************
# boolean value is used by both the cwbsnamapsd server process
# and other processes such as cwbadmin, cwbdiscover, dlsw and rsrb to
# add devices to the database.
# When adding a device to the database, this value is used to decide
# whether to do a DNS lookup on the name of the device being added,
# storing the DNS name in the DNS database table.
#
# cwbsnamapsd uses this value to decide whether to do a DNS lookup on
# a device name supplied in a user's request, if the request could
# not be satisfied with a device name or IP address lookup.
# The default value is "false", DNS lookups are not enabled. Set this
# value to "true" to enable DNS lookups.
doDNSSearch = false
```

You can set the *doDNSSearch* variable in the *cwbinit* file to **true** to discover and query routers by any valid name. Now you can enter the discovered name, a valid IP address, or any valid name for the router. For example, you could enter **cwb-c5** in the input field for a DLSw focus view even if the router was discovered as *cwb-c5.cisco.com*. To enable domain name server lookup for routers, change the doDNSSearch value to **true**:

```
doDNSSearch = true
```

The DNS lookup is performed when the router is added to the database and any time a device cannot be found by the discovered name or IP address. This lookup might impact performance.

Note After you change the *doDNSSearch* parameter, you should stop and restart *cwbsnamapsd*.

Changing the Local Workstation IP Address or Host Name

During installation, the CiscoWorks Blue products save the host name of the workstation in a set of files for use during processing. If you later change the host name of the workstation, you must also change the host name in those files.

To change the host name, use the following procedure:

Step 1 Use the following command to stop all CiscoWorks Blue processes:

/opt/CSCOcb/bin/cwb stop all

Step 2 Change the host name in the following files:

- */opt/CSCOcwbC/classes/com/cisco/nm/cmf/kubit/process/*
  - *PMInstall.properties*
  - *displayMain.properties*
  - *procMgrServer.properties*
  - *processCLI.properties*
- */opt/CSCOcwbC/classes/com/cisco/nm/cmf/kubit/logger/ logger.properties*
- */opt/CSCOcwbC/etc/*
  - *Services.conf*
  - *runprocess*
- */opt/CSCOcwbC/apache/etc/httpd.conf*
- */opt/CSCOcwbC/db/ctlibs/interfaces*

Step 3 Use the following command to restart all Cisco Works Blue processes:

/opt/CSCOcb/bin/cwb start servers

The CiscoWorks Blue products do not include the local workstation's IP address in any of its files, so you can change without impact.

Using the Process Manager

This chapter provides information on using the Process Manager on a UNIX workstation. The CiscoWorks Blue Process Manager provides an interface for starting, monitoring, and stopping the Maps and SNA View daemons and processes and the Process Manager services.

The Process Manager starts automatically when your system starts. When the Process Manager starts, it starts all the Maps and SNA View processes that are marked as Autostart, and it restarts any processes that have been stopped abnormally and are marked for Restart.

This chapter includes the following main sections:

Starting the Process Manager

This section describes how to start the Process Manager. The Process Manager consists of a server component that monitors and maintains the running processes and a client component that displays the results in a graphical user interface.

This section includes the following information:

Starting the Server Components

CiscoWorks Blue server processes are normally started automatically and kept running. Should you need to manually start them, use the following commands on a UNIX workstation:

From the command line, use the **cwb start servers** command to start all CiscoWorks Blue servers, including the database server and the Process Manager server. Because starting the database and naming servers requires root authority, you should always run **cwb start servers** as the root user:

/opt/CSCOcb/bin/cwb start servers

From the command line, use the **cwb start pm** command to start the Process Manager server:

/opt/CSCOcb/bin/cwb start pm

Starting the Client Component

You can start the Process Manager client from the Administration application or from the command line. From the command line, use the **cwb start ProcMgrClient** command:

/opt/CSCOcb/bin/cwb start ProcMgrClient

From the Administration application, click **Process Manager**.

Viewing the Process Management Information Window

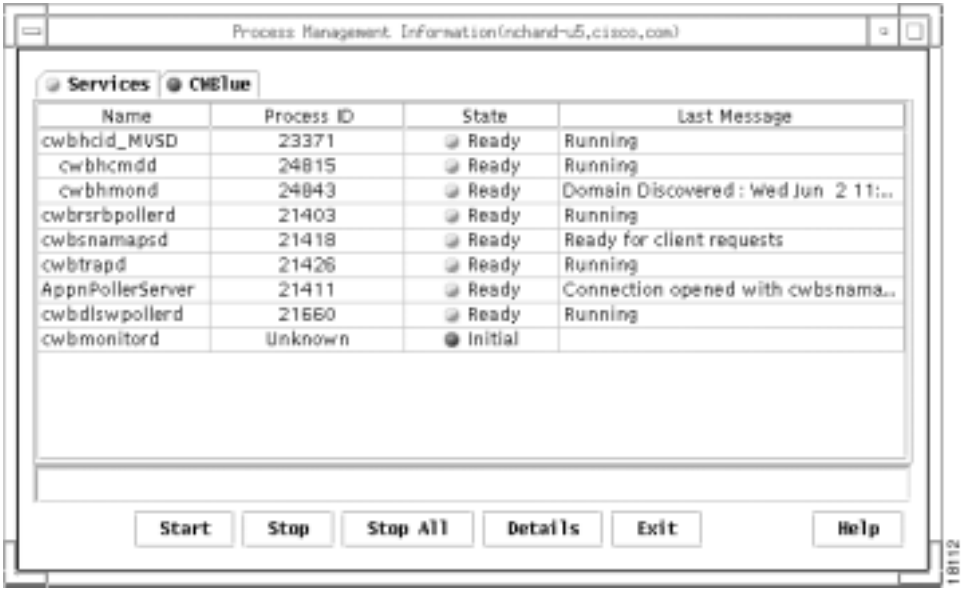
The Process Management Information window contains two tabs:

- The CWBlue tab displays the Process Management Information—CWBlue window. This window displays all the Maps and SNA View processes configured to run under Process Manager.
- The Services tab displays the Process Management Information—Services window. This window displays the Process Manager services.

Viewing the Process Management Information CiscoWorks Blue Window

The CWBlue window displays a list of the Maps and SNA View processes in a single window, as shown in Figure 5-1. The host name of the connected workstation is displayed in the title bar of the window.

Figure 5-1 Process Management Information—CWBlue Window



Fields

The CiscoWorks Blue window contains the following fields:

Field	Description
Name	The name of this process. See the "Maps and SNA View Daemons and Processes" section on page 5-7.
Process ID	A number identifying a process that is running.

Field	Description
State	Status of this process. The status colors are as follows: • Green means the process is currently active. • Blue means the process is in its initial state and has not been started. • Red means the process has been run and then stopped. • Yellow means the process is being started or stopped.
Last Message	Last message issued by this process. This is usually a status message that tells you what the process did last or why the process stopped.

Buttons

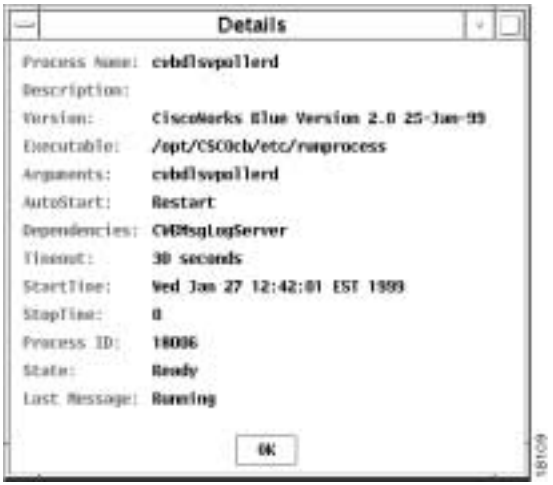
The buttons on the CiscoWorks Blue window provide the following functions:

Button	Description
Start	Starts the selected process.
Stop	Stops the selected process.
Stop All	Stops all running processes.
Details	Displays the Details window (Figure 5-2) for the selected process.
Exit	Stops the Process Manager client and closes the window.
Help	Displays the online help.

Viewing the CiscoWorks Blue Details Window

You can see detailed information about each process. Select a process and click **Details** in the CiscoWorks Blue window to view the details of the selected process. The Details window is displayed, as shown in Figure 5-2.

Figure 5-2 CiscoWorks Blue Details Window



Fields

The Details window contains the following fields:

Field	Description
Process Name	Name of the Maps process, as listed in the "Maps and SNA View Daemons and Processes" section on page 5-7.
Description	Description of the process.
Version	Version of the process.
Executable	Full path name for the executable file for the process.
Arguments	Command line switches for the process.

Field	Description
Autostart	Indicates whether the process is configured to start automatically: • **Yes** means it will be automatically started. • **No** means that it will not be automatically started unless some other process is dependent on it. • **Restart** means that it will be automatically started and, if it stops abnormally, it will be restarted automatically. However, if you use the Process Manager to stop this process, it will not be restarted automatically.
Dependencies	Lists processes that must be running before this process is started.
Timeout	Time that the Process Manager waits for an Initialization Complete notification from the started process.
Start Time	Date and time that the process was last started. If the process was never started, this field is 0.
Stop Time	Date and time that this process was stopped. If the process is currently running, this field is 0.
Process ID	Process ID of the named process.
State	Status of the process.
Last Message	Last message sent by the process to the Process Manager.

Maps and SNA View Daemons and Processes

The following table shows the Maps and SNA View daemons and processes that can be monitored in the Process Manager:

Process Name	Description
cwbrsrbpollerd	RSRB Poller daemon, which polls RSRB MIBs.
cwbdlswpollerd	DLSW Poller daemon, which polls DLSw MIBs.
cwbmonitord	Monitor daemon, which updates Maps Motif applications with changes.

Process Name	Description
cwbtrapd	Trap daemon, which registers with the network management system (NMS) trap process.
cwbsnamapsd	CiscoWorks Blue Web daemon, which gets requested database information for the web server.
cwbhcid_*domain_name* cwbhcid_server_*domain_name* cwbhcmd_server_*domain_name*	SNA View host connection interface, which gets messages from the mainframe host. The cwbhcid (tcp) and cwhci_server(lu62) tasks will have multiple entries in the *CWBlue.conf* file, one for each domain. The process name for each entry has the domain name appended. Only one domain is supported for LU 6.2.
cwbhcmdd	TCP/IP version of SNA View host command server daemon, which sends commands to the mainframe host. There is an instance of cwbhcmdd for each domain.
cwbhmond	TCP/IP version of SNA View monitor/discover daemon. There is an instance of cwbhmond for each domain.

Note The cwbhcmdd and cwbhmond TCP/IP processes are transient daemons. They are started by cwbhcid_*domain_name*, not by the Process Manager. Once started, their status is displayed by the Process Manager. When cwbhcid stops, these two stop as well, and disappear from the Process Manager window.

Automatic Starts and Dependencies

Depending on the selections you make during configuration, some processes are set up to start automatically when the Process Manager starts, and some processes are dependent on others.

Autostarted Processes

Depending on your configuration options, the following processes are started automatically:

Configuration Option	Processes Autostarted
DLSw	cwbdlswpollerd and cwbtrapd[1] start automatically.
RSRB	cwbrsrbpollerd and cwbtrapd[1] start automatically.
TCP host connection	cwbhcid starts automatically. If you configure an LU 6.2 host connection, you must configure the LU 6.2 transaction programs. The SNA mainframe application will then cause cwbhcid_server_domain to start.

1. The cwbtrapd process is started only if an NMS was integrated during installation.

Dependent Processes

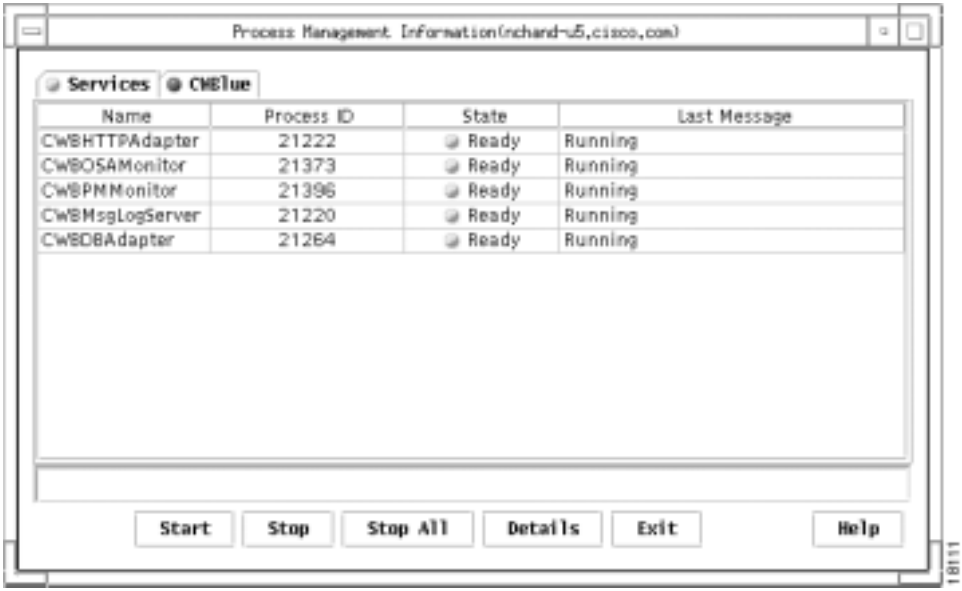
The following processes start only after other processes are started:

Process	Depends on
cwbmonitord	CWBMsgLogServer, CWBDBAdapter
cwbhcid cwbhcid_server_*domain*	CWBMsgLogServer, CWBDBAdapter
cwbsnamapsd	CWBMsgLogServer, CWBDBAdapter
cwbdlswpollerd	CWBMsgLogServer, CWBDBAdapter
cwbrsrbpollerd	CWBMsgLogServer, CWBDBAdapter
cwbtrapd	CWBMsgLogServer, CWBDBAdapter

Viewing the Process Management Information Services Window

The Services window displays a list of all the Process Manager services, as shown in Figure 5-3.

Figure 5-3 Process Management Information—Services Window



Fields

The Services window contains the following fields:

Field	Description
Name	Name of the service.
Process ID	Process ID of the service.
State	Current service status. The status colors are used as follows: • Green means the service is currently active. • Blue means the service is in its initial state and has not been started. • Red means the service has been run and then stopped.
Last Message	Last message sent by the service.

Buttons

The buttons on the Services window provide the following functions:

Button	Description
Start	Starts the selected service.
Stop	Stops the selected service.
Stop All	Stops all running services.
Details	Displays the Details window for the selected service, as shown in Figure 5-4.
Exit	Stops the Process Manager client and closes the window.
Help	Displays the online help.

Viewing the Services Details

You can see detailed information about each service. From the Services window, select a service and click **Details** to view the Services Details window for the selected service, as shown in Figure 5-4.

Figure 5-4 Services Details Window

Fields

The Services Details window contains the following fields:

Field	Description
Process Name	Name of the Services process, as described in "Process Manager Services, page 5-13."
Description	Description of service.
Version	Version of the process.
Executable	Full path name for the executable file for the process.
Arguments	Command line switches for the process.
Autostart	Indicates whether the process is configured to start automatically: • **Yes** means it will be automatically started. • **No** means it will not be automatically started unless some other process is dependent on it. • **Restart** means it will be automatically started and, if it stops abnormally, it will be restarted automatically. However, if you use the Process Manager to stop this process, it will not be restarted automatically.
Dependencies	Lists processes that must be running before this service can be started.
Timeout	Time that the Process Manager waits for an Initialization Complete notification from the started process.
StartTime	Date and time that the process was last started. If the process was never started, this field is 0.
StopTime	Date and time that this process was stopped. If the process is currently running, this field is 0.
Process ID	Process ID of the named process.
State	Status of the process.
Last Message	Last message sent by the process to the message log.

Process Manager Services

The following Process Manager services can be monitored in the Services window:

Process Name	Description
CWBMsgLogServer	Message log server logs messages from the Maps and SNA View applications and daemons. To view the messages, use the message log viewer (**cwb start MsgLogClient**).
CWBHTTPAdapter	Starts and monitors the web server.
CWBOSAMonitor	Monitors the osagent process, which provides CORBA naming services.
CWBDBAdapter	Starts and monitors the database servers.
CWBPMMonitor	Monitors the Process Manager server. If the Process Manager server dies, this process stops all Maps processes and restarts the Process Manager server.

Automatic Starts and Dependencies

Depending on the selections you make during configuration, some services are set up to start automatically when the Process Manager starts, and some services are made to be dependent on others.

Autostarted Processes

The following services are started automatically when the Process Manager server starts:

- CWBMsgLogServer
- CWBDBAdapter
- CWBHTTPAdapter

Dependent Processes

The following services start only after other processes are started:

Process	Depends On
CWBMsgLogServer	Nothing
CWBDBAdapter	CWBMsgLogServer
CWBHTTPAdapter	CWBMsgLogServer

Configuring the Process Manager

This section provides information about the different ways you can configure how the Process Manager runs.

Monitoring the Process Manager

The CWBPMMonitor process monitors the Process Manager to ensure that it remains active. If the Process Manager is not running, the CWBPMMonitor process stops all other CiscoWorks Blue processes. It then restarts the Process Manager server which in turn starts all the other servers.

Use the *CWBProcessMgrWaitTime* parameter in the */opt/CSCOcb/etc/cwbinit* file to specify how often, in minutes, the CWBPMMonitor process wakes up to check whether the Process Manager is running. The default value is 10 minutes.

```
**************************************************************

# This section is used by the Process Manager monitor process, which
# monitors the state of the CiscoWorks Blue Process Manager.
# This parameter controls how often, in minutes, the CWBPMMonitor
# process wakes up and makes sure that the Process Manager process is
# running on the system. If it is not running, this process stops
# all CWBlue processes and restarts Process Manager, which restart
# all servers.
CWBProcessMgrWaitTime = 10
```

Use the *showWarnings* parameter in the */opt/CSCOcb/etc/cwbinit* file to specify whether the Verification program should issue warning messages.

```
**********************************************************************
# This section is used by the Verification Utility which validates
# the CiscoWorks Blue installation.
# Flag indicating whether or not the verification utility should issue
# warnings. If "true" warnings are issued, "false" otherwise.

showWarnings = true
```

Configuring Process Manager Windows

The Process Manager is configured, during Maps or SNA View installation, to monitor the complete set of processes and to automatically start those processes that support the protocols (DLSw, APPN/SNASw, and RSRB) that you want to manage. The settings that govern the Process Manager are stored in the following configuration files in */opt/CSCOcwbC/etc*:

- *CWBlue.conf* contains the settings for monitoring processes common to both Maps and SNA View.
- *Services.conf* contains the settings for monitoring services, such as the message log server.

Normally you would not need to make any changes in these configuration files. However, you might want to change selected default values (such as the Autostart value) or process dependencies.

The *CWBlue.conf* configuration file contains entries that describe the Maps and SNA View processes to be monitored and managed by the Process Manager. The *Services.conf* file contains entries that describe the Process Manager services to be monitored and managed by the Process Manager. Each file is made up of a series of entries, one for each process or service. Each entry is in the following format:

```
process_name autostart? dependencies executable arguments time_out
```

The entry contains the following fields:

Entry	Description
process_name	Name of the process or service.
autostart?	Indicates whether the process is to start automatically: • **Y** means it is started automatically. Process Manager will try to autostart this process once. • **N** means it is not started automatically. • **R** means it is started automatically and, if it is killed, it is restarted automatically. Process Manager tries to autostart this process for some period. However, if you use Process Manager to stop this process, it is not restarted automatically.
dependencies	One or more process names separated by commas (,). Each dependent process in the list must be started before the subject process is started. If there are no dependencies, use one hyphen (-) as a place holder.
executable	Complete directory path and executable command.
arguments	Set of command-line arguments (switches) and their associated values separated by commas (,) that the Process Manager will use to start the process.
time_out	Time the Process Manager waits for a notification from the application. When the time expires, the Process Manager does not change the starting state. It reports a timeout error.

Sample CWBlue.conf File

The following sample *CWBlue.conf* file shows the file contents after you install CiscoWorks Blue:

```
# The Process Manager Configuration File for Maps/SNAView processes.
# Each line contains 6 tokens separated by spaces

# Format:
# process_name AutoStart Dependencies Executable Args TimeOut

# process_name :Name of the process

# autoStart :(Y/N) Whether ProcessManager should automatically
# [re]start this process

# Dependencies :(A list of process_name each separated by ',')
# Each process in the list has to be started before the particular # #
# process can be started. If there are no dependencies, a single '-'
# is used.

# Executable :Complete path to the executable representing the process

# Args :Arguments to the process, separated by ',' ; If no arguments #
# are required, a '-' should be specified.

# TimeOut :(timeout value) The time in seconds, until which the PM
# waits for a 'InitializationComplete' notification from the
# started process). Once it receives the notification, the state of
# the process is moved from starting->Ready.

cwbmonitord N CWBMsgLogServer,CWBDBAdapter /opt/CSCOcb/etc/runprocess
cwbmonitord 30

cwbhcid_MVSD R CWBMsgLogServer,CWBDBAdapter /opt/CSCOcb/etc/runprocess
cwbhcid_MVSD,MVSD 30

cwbsnamapsd R CWBMsgLogServer,CWBDBAdapter /opt/CSCOcb/etc/runprocess
cwbsnamapsd 30

cwbdlswpollerd R CWBMsgLogServer,CWBDBAdapter
/opt/CSCOcb/etc/runprocess cwbdlswpollerd 30

cwbrsrbpollerd R CWBMsgLogServer,CWBDBAdapter
/opt/CSCOcb/etc/runprocess cwbrsrbpollerd 30
```

Sample Services.conf File

The following sample *Services.conf* file shows the file contents after you install CiscoWorks Blue on a UNIX workstation:

```
CWBMsgLogServer R - /opt/CSCOcwbC/bin/CWB_msgLogServer
-MLCname,CWBMsgLogServer,-N,CWBMsgLogServer,-PMCname,CWBMsgLogServer,-
MLCserverName,CWBMsgLogServer,-F,cwblogger.log,-P,/opt/CSCOcb/logs,-PM
CserverName,CWBProcessMgr,-ORBagentPort,44542

CWBDBAdapter R CWBMsgLogServer /opt/CSCOcb/etc/runprocess
CWBDBAdapter 100

CWBHTTPAdapter R CWBMsgLogServer /opt/CSCOcb/etc/runprocess
CWBHTTPAdapter 70

CWBOSAMonitor R CWBMsgLogServer /opt/CSCOcb/etc/runprocess
CWBOSAMonitor 50

CWBPMMonitor Y CWBMsgLogServer /opt/CSCOcb/etc/runprocess
Changing Maps Processes and Services
```

After you make changes to the *Services.conf* or *CWBlue.conf* configuration file, you must activate those changes by stopping and restarting the Process Manager server, as described in "Starting the Process Manager, page 5-1." The Process Manager restarts, starting any processes specified as **autostart** in the changed configuration file.

Restarting the Process Manager

Use the following information for the different ways you can start the Process Manager servers and client on UNIX Workstations.

Process Manager Server

After you stop the Process Manager server, you can restart it from the command line using the following commands:

/opt/CSCOcb/bin/cwb start pm

Process Manager Client

Restart the Process Manager client from the command line using the following command:

/opt/CSCOcb/bin/cwb start ProcMgrClient

Changing Process Manager Properties

You can edit the Process Manager properties file to change Process Manager properties.

The file is */opt/CSCOcwbC/classes/com/cisco/AM/conf/kubit/process/displayMain.properties*.

You can change the following values:

Value	Meaning
WriteAccess	true—Runs the Process Manager client in read/write mode so that the Process Manager client can display processes and can start or stop processes. false—Forces the Process Manager client into read-only mode so that the Process Manager client can display processes, but cannot start or stop processes.
PromptUser	true—Prompts the user when stopping Process Manager. false—Suppresses the prompt when stopping Process Manager.

Using the Message Log Viewer

This chapter provides information on using the Message Log Viewer. The CiscoWorks Blue Message Log Viewer consists of a message log server and a message log client. The CiscoWorks Blue Process Manager automatically starts the message log server, which collects error messages from all the Maps and SNA View processes and stores them in the message log. You can view the messages from the Message Log viewer.

This chapter includes the following main sections:

Getting started

Use the following information to start the Message Log.

- The message log client lets you view the messages as they are logged. To start the message log client, use the **cwb start MsgLogClient** command:

  /opt/CSCOcb/bin/cwb start MsgLogClient

- From the Administration window, select **Tools > Message Log Client**

Note The message log client displays messages only while they are being logged and the message log client is active. It does not display messages from the message logs themselves. To see any messages that were logged before you started the message log client, view the message log files as described in the "Viewing the Message Logs" section on page 6-16.

Displaying a Message Log View

You can view messages that meet the criteria defined for each view you create. A default view, called **All**, displays all the messages that are being logged. To define your own customized views, see the "Customizing a Message Log View" section on page 6-3.

Note Normally you should use the All view because the other views are temporary and are not saved when you exit the Message Log application.

Step 1 Display the Message Log Information window. The Log Control window is displayed.

Step 2 Click the **Log Display** tab. The Log Display window is displayed.

Step 3 In the Log Display window, click the button for the view you want to see. Figure 6-1 shows only one view button, **All**. Click **All** to see all the logged messages. Click another view button, if available, to see the messages logged for that view.

Figure 6-1 Message Log Information—Log Display Window

Customizing a Message Log View

The default view, named All, shows all messages being logged. You can use the New View window to create customized views showing data that meet specific criteria. For example, a view that shows messages from only a small set of applications or that displays only selected key message fields.

Note This New View is temporary and is removed when you exit the Message Log Client.

To customize message views, specify a set of criteria for selecting the messages you want to view and for determining how much information about each message you want to see.

For details about each field, see the "Using the Message Log New View Window" section on page 6-11.

Step 1 Display the Log Display window using the procedures for the "Displaying a Message Log View" section on page 6-2. The Log Control window is displayed.

Step 2 Click **Log Display**. The Log Display window is displayed.

Step 3 In the Log Display window, click **New View**. The New View Display window is displayed, as shown in Figure 6-2.

Figure 6-2 Message Log New View Window

Step 4 In the Enter view name field, enter a name for this view. It should be short enough to fit on a view button.

Step 5 In the Specify filter for the log messages field, click **Enable** to enable filtering. Use the three following fields to create the message filter:

- Use the left field to specify the message characteristic that you want to filter.
- Use the center field to specify the message condition that you want to satisfy.
- Use the right field to specify the text that is the criteria of the filter.

Step 6 In the Specify fields to be displayed field, select the message elements that you want displayed for each message.

Step 7 In the Allow automatic clearing of message display field, specify the maximum number of messages that can accumulate in the message log for this view before the log is purged and new messages are logged.

Step 8 In the Highlighting field, click **Enable** to enable highlighting of messages that meet specified criteria. All messages that meet the criteria will be displayed in the selected color. Use the following three fields to create the highlighting criteria:

- Use the left field to specify the message characteristic that you want to filter.
- Use the center field to specify the message condition that you want to satisfy.
- Use the right field to specify the text that is the criteria of the filter.

Step 9 In the **Color** field, select the color to be used for highlighting.

Step 10 Click **OK** to save your changes. The message view appears as a button on the Log Display window.

Deleting a Message Log View

After you define a series of message views, the Log Display window may become cluttered with view buttons. To remove some of the buttons, use the following procedure:

Step 1 In the Log Display window, click the button for the view you want to delete. A large **X** appears in a square button at the upper-right corner of the message display just above the right scroll bar.

Step 2 Click the large **X**. The button for that view is deleted.

Using the Message Log Viewer

The Message Log Viewer provides a log of status messages generated by the Maps and SNA View applications. To access the Message Log Viewer window, issue the **cwb start MsgLogClient** command. The window appears with the host name in the title bar. The Message Log Viewer window contains the following tabs, which you can click to display the Log Display and the Log Control windows:

- Log Display
- Log Control

Log Display Window

The Log Display window displays a list of the accumulated messages from one message view, as shown in Figure 6-1.

Figure 6-3 Log Display Window

The Log Display window displays all the messages logged for the selected view.

Buttons

The Log Display window has buttons that provide the following functions:

Button	Description
All	Displays all messages generated by the message categories enabled in the Log Control window.
View *Name* (up to 6)	Displays buttons for the new message views that you define in the New View window.
New View	Displays the New View window, which allows you to specify criteria for the message to be displayed in the Log Display window.
Clear View	Removes all of the currently displayed messages from the view.

Button	Description
Pause View/Resume View	Stops scrolling of the messages as they are received. New messages are still received but the list does not scroll in the view.
Exit	Stops the Message Log client and closes the window.
Help	Displays help information about the window.

Log Control Window

The Log Control window, as shown in Figure 6-4, displays a list of all currently running Maps and SNA View applications for which messages can be collected in the message log, and the message categories available for each application.

Figure 6-4 Message Log Information—Log Control Window

You can change which message levels are logged by default for each process by editing the **runprocess** command script or by changing them in this window.

Editing the **runprocess** script is described in Appendix D, “CiscoWorks Blue Commands and Processes.”

Note For HP systems only, the APPN/SNASw, DLSw, RSRB, and PollerServer applications do not send messages to the Message Log server. Therefore, you cannot view messages from those applications in either the Message Log client or the message logs files.

The Log Control window contains the following fields:

Field	Description
Process Name	Lists, by name, all the currently running Maps and SNA View applications on UNIX workstations. You can change which message levels are logged by each process by editing the **runprocess** command script or by changing them dynamically here. Editing the *runprocess* script is described in Appendix D, "CiscoWorks Blue Commands and Processes."
Message Category	For the selected application, lists all valid message categories and indicates whether they are enabled for display. The message categories available include the following: **Debug**—Useful when you are debugging a problem with help from Cisco's Technical Assistance Center. **Error**—Generates messages when any operational error condition occurs. **Warning**—Generates messages when an error condition that is not fatal occurs. **Info**—Generates messages to notify you of status information. **Trace**—Generates detailed operational log messages. **SNMP Trace**—Generates detailed SNMP trace log messages. **UITrace**—Generates trace log messages from a user interface. **IPCTrace**—Generates detailed log messages for socket operations and interprocess communication. **Dump**—Generates very detailed information. **InternalTrace**—Generates internal operational log messages. The Error, Warning, and Info message categories are enabled by default. To enable a message category, click **Enable**. Click **Apply** when finished.

Buttons

The Log Control window has buttons that provide the following functions:

Button	Description
Reset	Resets each message category to its previous (Enabled or Disabled) state.
Apply	Executes changes that you have made to the messages categories.
Exit	Stops the Message Log client and closes the window.
Help	Displays information about the window.

Using the Message Log New View Window

The Message Log New View window lets you add a new view for the message log, as shown in Figure 6-2. The default view, named All, shows all messages being logged. You can use the New View window to create customized views that show specific sets of data. For example, you might want to create a view that shows messages from only a small set of applications or that displays only selected key message fields.

Figure 6-5 Message Log New View Window

Fields

The Message Log New View window contains the following fields:

Field	Description
Enter view name	Enter a new name for this new view. The new name will appear on a button on the Log Display window.
Specify filter for the log messages	Select the **Enable** check box to enable filtering of messages in the message display. Use the left field to specify the characteristic you want to filter: **Process Name**—Filters messages based on the name of the issuing process. **Hostname**—Filters messages based on the name of the issuing host. **Message Category**—Filters messages based on the category of the message. **Message**—Filters messages based on the actual text in the message. Use the center field to specify the message condition you want to satisfy: **equals**—Displays messages that exactly match the filtering criteria. **not equals**—Displays messages that do not match the message criteria. **contains**—Displays messages that partially satisfy the criteria. Use the right field to specify the text that is the criteria of the filter. For example, to display messages with message categories that contain the word “error” (as in Error messages) you would select this item: Message Category contains error

Field	Description
Specify fields to be displayed	Specifies the fields in the message that you want displayed. select the check boxes of the fields you want to include. Deselect the check boxes of fields you do not want displayed.
Allow automatic clearing of message display	Lets you specify automatic clearing of the message log after a specified number of messages have accumulated.

Field	Description
Highlighting	Select the **Enable** check box to enable highlighting of messages in the message display. Use the left field to specify the characteristic you want to filter: **Process Name**—highlights messages based on the name of the issuing process. **Hostname**—highlights messages based on the name of the issuing host. **Message Category**—highlights filters messages based on the category of the message. **Message**—highlights messages based on the actual text in the message. Use the center field to specify the message condition you want to satisfy: **equals**—highlights messages that exactly match the filtering criteria. **not equals**—highlights messages that do not match the message criteria. **contains**—highlights messages that partially satisfy the criteria. Use the right field to specify the text that is the criteria of the filter: For example, to highlight messages with message categories that contain the word “error” (as in Error messages) you would select these items: Message Category contains error.
Color	Lets you specify the color of the text and background that displays in the View name section of the main window.

Buttons

The New View window has buttons that provide the following functions:

Button	Description
OK	Saves the view definition as a button on the Log Display window.
Cancel	Cancels the view definition and returns to the Log Display window.

Viewing the Message Logs

The CiscoWorks Blue messages are logged in message log files stored in the */opt/CSCOcb/logs* directory. Each message log file name is in the format *cwblogger.log.X*, where *X* is either 0 or 1. Look at the time stamp to find the most recent log file. You can view these message log files with any editor or file browser (such as the **more** command). This file wraps at 10000 messages.

When the Message log server is stopped and restarted, it begins logging messages in the log file that contains the oldest messages.

CHAPTER 7

Using the Administration Application

This chapter provides information on using the Administration application on UNIX workstations. Use the CiscoWorks Blue Administration application to add, delete, modify, and discover devices in your CiscoWorks Blue database, and to select DLSw key devices. DLSw key devices are described in the "Specifying the Status of Aggregated Peers" section on page 7-14.

This chapter includes the following main sections:

Starting CiscoWorks Blue Administration

This section covers starting the CiscoWorks Blue Administration application. You can start the Administration application from the following locations:

- Network management system (NMS)

- Workstation system prompt
- Remote workstation

Starting Administration From a Network Management System

You can start the CiscoWorks Blue Administration application from a NMS, such as NetView for AIX.

- On SunNet Manager select, **Tools > CWB-Administration** from the menu bar.
- On HP-OV and NetView for AIX, select **CWBlue > Administration** from the menu bar.

Starting Administration From a System Prompt

On a UNIX workstation, the CiscoWorks Blue Administration application is accessible from */opt/CSCOcb/bin/*. To start the application from a system prompt, enter the following commands:

cd /opt/CSCOcb/bin

./cwb start admin

Starting Administration From a Remote Workstation

You can log in to a remote UNIX host from your own local UNIX workstation, export the remote host display to your local workstation, and then run the application from the remote host. To start the remote host's CiscoWorks Blue Administration application from your local workstation, use the following procedure:

Step 1 At your local UNIX workstation, enter the following command:

xhost +

Step 2 Log in to the remote UNIX host as root (or with a username of your own choosing).

Step 3 Set your DISPLAY environment variable to export the display from the remote host to your local workstation. Depending on which shell you are using, use one of the following commands:

- From the K shell (ksh):

  setenv DISPLAY

  export DISPLAY=*IP_address***:0.0**

- From the C shell (csh) or TC shell (tcsh):

  setenv DISPLAY *IP_address***:0.0**

Step 4 To start the CiscoWorks Blue Administration application, enter the following commands:

cd /opt/CSCOcb/bin

./cwb start admin

Using the Main Administration Window

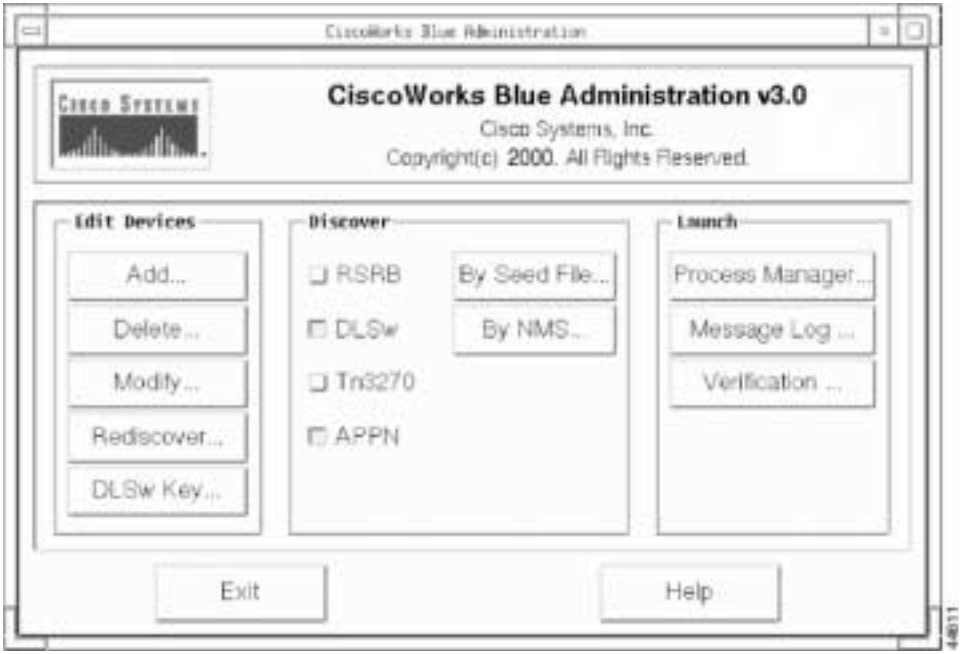
When you start the CiscoWorks Blue Administration application, the CiscoWorks Blue Administration window is displayed. Use the CiscoWorks Blue Administration window to add, delete, modify, and discover devices in your CiscoWorks Blue database, and to select DLSw key devices.

Use the main window to perform the following tasks:

- Discovering devices by seed file
- Discovering devices by NMS
- Adding devices
- Deleting devices
- Modifying devices
- Rediscovering devices
- Selecting DLSw key devices

Main Administration Window

Figure 7-1 CiscoWorks Blue Administration Window



Edit Devices Area

The Edit Devices area allows you to manipulates the devices in the database and includes the following buttons:

Buttons

The Edit devices area has the following buttons:

Button	Description
Add	Add adds one or more devices, separated by spaces, to the database.
Delete	Delete deletes one or more devices from the database.

Button	Description
Modify	Modify changes the read community string for one or more devices.
Rediscover	Rediscover rediscovers one or more devices in the database.
DLSw Key	DLSw Key designates or removes one or more devices as DLSw key devices

Discover Area

The Discover area allows you to discover DLSw, RSRB, APPN/SNASw, or TN3270 devices using either a seed file or an NMS database, and adds the discovered devices to the CiscoWorks Blue database. Discover performs a common discovery process, which includes any SRB rings. Discover queries routers for the protocols you select.

Buttons

The Discover area has the following buttons:

Button	Description
RSRB	RSRB discovers RSRB devices.
DLSw	DLSw discovers DLSw devices.
TN3270	TN3270 discovers TN3270 devices. (To use this function, you must have a valid license for the SNA View application.)
APPN/SNASw	APPN discovers APPN/SNASw devices.

Check Boxes

The Discover list includes the following check boxes:

Check Box	Description
By Seed File	By Seed File starts discovery using a seed file. You are prompted for the seed file name.
By NMS	By NMS starts discovery using an NMS database. (This option is available only when an NMS was selected during installation.)

Launch Area

The Launch area allows you to start CiscoWorks Blue client applications:

Buttons

The Launch area has the following buttons:

Button	Description
Process Manager	Process Manager starts the Process Manager client application.
Message Log	Message Log starts the Message Log viewer client application.
Verification	Verification starts a web browser and displays the Verification web page.

Administration Window

Buttons

The Administration window has the following buttons:

Button	Description
Exit	Exits the CiscoWorks Blue Administration application.
Help	Displays online help in a web browser window.

Buttons in Other Windows

Buttons

Other windows in the Administration application may have one or more of the following buttons:

Button	Description
OK	Designates the devices in the Selected list as DLSw key devices. The devices in the Devices list remain unchanged.
Cancel	Cancels the operation and returns to the previous window.
Help	Displays online help for the Key Device Selection window.
<< and >>	Moves devices between the Devices list and the Selected list.

Discovering the Network

This section covers how to discover the various protocols in your networks:

- Discovering DLSw Devices in the Network, page 7-9
- Discovering RSRB in the Network, page 7-18
- Discovering APPN/SNASw in the Network, page 7-23

Discovering DLSw Devices in the Network

This section describes how to discover the Cisco DLSw-enabled routers in your SNA network.

Discovery is the process by which the DLSw application queries each device in the network to determine whether it is enabled for DLSw networking. Each time the DLSw application finds a router, it performs one of the following actions:

- If the router is enabled for DLSw and SNMP, the discover process adds the router name as a DLSw router in the database, and it polls that router.
- If the router is not enabled for DLSw, the discover process stores that router name as a non-DLSw router in the database, and it does not poll that router. Every time the process runs, it tries to discover these non-DLSw routers.
- If a router cannot be accessed by SNMP, the discover process tries to reach that router each time discovery is run.

There are several ways in which the DLSw application can discover the routers in a network. You can provide a list of enabled routers in a special file called a seed file. Or you can let the Maps application get its information from an NMS database.

Both methods of discovery are described in the following subsections:

- Discovering the Network with a Seed File, page 7-9
- Discovering the Network with a Network Management System Database, page 7-12
- Discovering Individual DLSw Routers, page 7-13
- Rediscovering Individual DLSw Routers, page 7-13
- Correlating SNA Resources with DLSw Routers, page 7-14

Discovering the Network with a Seed File

If your NMS is incapable of providing an accurate list of Cisco routers, or if you want to provide a list of routers to limit discovery, you can create a seed file for the Maps application.

Seed File Format

Each record in the seed file can be either a comment or a router specification. You can list the routers in any order within the seed file.

A comment is a single line of text that begins with the pound (#) character, as shown below.

```
# This line is a comment.
A router specification can have one of the following formats:
router [ReadCommunityString] [key]
```

or

```
router:[ReadCommunityString]:[key]
```

Use the following conventions for the router specification:

- The delimiter can be a space or a colon (:).
- *router* can be either a host name or the IP address of a DLSw-enabled router in the network. This is the same label that marks the router on a map.
- *ReadCommunityString* is the read community string for the router. If you do not include this, the default read community string of "public" is used. If you want to designate this router as a key device while still using the default read community string, use the asterisk (*) to represent the default read community string (public). You can omit this value if you do not want to use the key value.
- *key* indicates that this is a DLSw key device. If you omit the word "key," the router is not considered a DLSw key device. This option is used only by the DLSw application. It is ignored by APPN/SNASw, RSRB, and TN3270. For information about key devices, read the "Specifying the Status of Aggregated Peers" section on page 7-14 and the "Define Key Devices" section on page 2-18.

Sample Router Specification in a Seed File

The following sample router specification designates router west.cisco.com as a key device with the read community string "public":

```
west.cisco.com:public:key
```

Cross-Application Use

Because the *key* parameter is used only for DLSw and is ignored for APPN/SNASw and RSRB, you can use the same seed file for all three Maps applications. The following lines are from a sample seed file:

```
# Seed file for CiscoWorks Blue Maps applications
# Next is a non-key router with goldilocks read community string
east.cisco.com goldilocks
# Next is a non-key router with default read community string
172.18.7.47
# Next is a key router with default read community string
west.cisco.com:*:key
# Next is a key router with a read community string
east.cisco.com:readstring:key
```

Note Do not allow any extraneous characters, spaces, or blank lines in your seed file. They can cause database problems. Also, remember that the device names and read community strings are case-sensitive.

Using the Seed File for Discovery

To use a seed file to provide the information to the application, use the following procedure:

Step 1 Use a text editor to create the seed file. Save the seed file, for example with the name *dlswseed*.

Step 2 Start DLSw and select **Admin > Discover > Seed File** to display the Seed File Discover window.

Or you can use the CiscoWorks Blue Administration application, as described in Chapter 7, “Using the Administration Application.”

Step 3 Enter the name of the seed file, verify the correct read community string, and click **Discover**. Discovery takes place while you wait.

After loading the database using the seed file, the DLSw application operates normally until a router is taken off line or a new router is configured. At that time, you can perform one of the following actions:

- Create a new seed file for the new router.
- Add the new routers to the existing seed file and rerun discovery from the seed file. DLSw ignores already discovered routers and discovers just the added routers.
- Add one or more devices directly to the global map, as described in *CiscoWorks Blue Maps and SNA View User Guide*.

Discovering the Network with a Network Management System Database

The NMS maintains a database, which includes all SNMP-managed routers in your network. You can use that database to provide the Maps application with the information it needs to discover the DLSw-enabled routers in the network. You can do this manually or automatically.

Discovering the Network Manually

To have the Maps application discover the network from the NMS database manually, select **Admin > Discover > Database** from the Maps application menu bar. The Maps application adds the routers found by the NMS to the database. The Maps application checks the database for new routers, polls their MIBs, and updates the database with the new MIB information.

Discovering the Network Automatically

You can have Maps check the NMS database automatically. This is called automatic discovery mode; you might want to use it if you expect to install or reconfigure routers often. To use automatic discovery mode, use the **cwb start cwbdiscover** command as a UNIX *cron* job (a chronologically started job). Set the cron job to run at night or when system and network activity are low.

Discovering Individual DLSw Routers

If you want to add only one or a few routers to your network, you can discover each router individually using the following procedure:

Step 1 Select **Edit > Add Device(s)**.

Step 2 When prompted, enter the router's device name and its read community string.

Step 3 Click **OK**.

The DLSw application adds the router to the database, polls the router's MIB, and adds the MIB information to the database. Watch the status area to see a message indicating the success or failure of this polling.

Rediscovering Individual DLSw Routers

It is sometimes useful to rediscover a DLSw router, especially if one of the following events occurs:

- A message appears in the status area indicating that the device already exists in the database.
- A router was just configured with DLSw.
- A later version of the Cisco IOS software was installed on the router, and the DLSw MIB is now supported.
- Router interfaces have been reconfigured.

There are several ways to rediscover individual routers:

- You can select **Edit > Rediscover Device(s)** from the DLSw menu bar.
- You can select a router icon on the map, click the right mouse button, and select **Rediscover** from the popup menu.
- You can use the Administration application.

Correlating SNA Resources with DLSw Routers

The following conditions must be met to have SNA PUs and LUs correlated with the DLSw routers that support them:

- The DLSw Maps application must poll routers for the DLSw circuits to obtain the latest SNA information.
- At least one of the polled routers, through which a circuit passes, must be designated as a key device.

Specifying the Status of Aggregated Peers

In a key devices view of the network, each key router is shown connected to one icon that represents all of that router's peers. This icon is called an aggregated peer router. The connection from the key router to its aggregated peer router is called an aggregated peer connection. Each aggregated peer connection and each aggregated peer router is displayed in a color that indicates its status. The status shown for the aggregated peer or peer connection represents the status of each component that makes up the aggregate. You can specify how to choose the color in which the aggregated status is displayed. There are two ways to choose the status of an aggregated peer or peer connection: using the worst-case status or using a calculated status.

Note The method that you select for specifying the status of aggregated peers affects all aggregates on the map.

Using the Worst-Case Status

You can choose to have all aggregated peers displayed in the color that is used for the peer with the worst status. For example, if the worst peer connection represented in the aggregated peer connection is inactive, then the aggregated peer connection is displayed as a red line and its aggregated peer router is also displayed in red.

To specify how aggregated peers are displayed, use the following procedure:

Step 1 Select **Edit > Define Aggregate Status** from the menu bar. The Aggregate Status Definition window is displayed.

Step 2 Select **Propagate Highest Abnormal Status**.

Step 3 Click **Apply**.

Using a Calculated Status

A peer connection can have one of four statuses: active, degraded, inactive, or unknown. Degraded, and inactive statuses are considered abnormal. When all peer connections have unknown status, the aggregate status is "unknown."

You can choose to have the aggregated peers displayed in a color that represents a status calculated from that of the individual peers which make up the aggregation. The calculation is based on the percentage of peers in the aggregation whose condition is abnormal. An abnormal condition is based on the reported status of the peer.

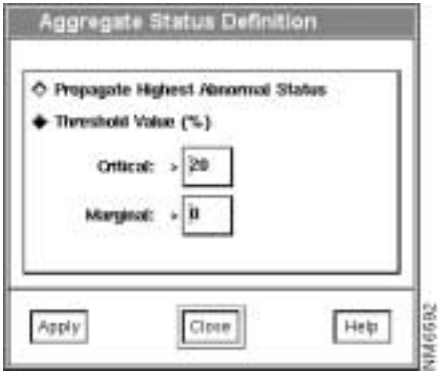
To determine how to display an aggregated peer, look at the percentage of individual peers with an abnormal condition in the aggregated peer. Once that percentage is determined, you define two threshold values: the Marginal% value and the Critical% value.

Specifying the Threshold Percentages

To specify percentages for the Marginal% value and Critical% value, use the following procedure:

Step 1 From the menu bar, select **Edit > Define Aggregate Status**. The Aggregate Status Definition window is displayed, as shown in Figure 7-2.

Figure 7-2 Aggregate Status Definition Window



Step 2 Select **Threshold Value (%)** and enter the values in the **Critical%** and **Marginal%** fields.

Step 3 Click **Apply**.

Defining the Marginal% Threshold

The Marginal% value is a threshold value that the DLSw application uses to determine which aggregated peers are in a degraded state or an active state. When the percentage of abnormal peers in the aggregation exceeds this threshold value, the aggregated peer status is considered degraded and is displayed in yellow. When the percentage of abnormal peers in the aggregation is less than or equal to this Marginal% value, the aggregated peer status is considered active and is displayed in green.

You define the Marginal% value for your network. The default Marginal% value for DLSw aggregated peers is 0 percent.

Defining the Critical% Threshold

The Critical% value is a threshold value that is used to determine which aggregated peers are in the inactive state. When the percentage of abnormal peers in an aggregation exceeds the critical% threshold value, the aggregated peer status is considered inactive and is displayed in red.

You define the Critical% value for your network. The default Critical% value for DLSw aggregated peers is 20 percent.

A special case occurs when all peers are unknown. In this case, the aggregated peer is considered unknown and is displayed in blue.

Calculating the Status for Peer Connections

DLSw calculates the status of an aggregated peer connection using the following method:

Step 1 DLSw finds the percentage of all peer connections in the aggregation whose status is abnormal. For this example, let *x* percent be the percentage of abnormal peer connections.

Step 2 DLSw compares the percentage of abnormal peer connections (*x* percent) to the Critical% value and to the Marginal% value.

Step 3 DLSw now calculates the status of the aggregated peer connection.

- If *x* percent is greater than or equal to 0 percent, but less than or equal to the Marginal% value, then the aggregated peer connection is considered active and is colored green.
- If *x* percent is greater than the Marginal% value, but less than or equal to the Critical% value, then the aggregated peer connection is considered degraded and is colored yellow.
- If *x* percent is greater than the Critical% value, then the aggregated peer connection is considered inactive and is colored red.

For example, there is a key router with six peer connections: three connections are active; one connection is unknown; and two connections are inactive. That means that 50 percent of the peer connections have abnormal status. Here are some scenarios:

- If we set the Marginal% value to 0 percent and the Critical% value to 20 percent (which are the default values), the 50 percent abnormal number falls above the Critical% value. The status of the aggregated peer connection is inactive and is displayed in red.
- If we set the Marginal% value to 30 percent and the Critical% value to 80 percent, the 50 percent abnormal number falls between the Critical% value and the Marginal% value. The status of the aggregated peer connection is degraded and is displayed in yellow.
- If we set the Marginal% value to 60 percent and the Critical% value to 80 percent, the 50 percent abnormal number falls below the Marginal% value. The status of the aggregated peer connection is active and is displayed in green.

Discovering RSRB in the Network

This section describes how to discover the RSRB-enabled routers in your SNA network. Discovery is the process by which the RSRB application queries each device in the network to determine whether it is enabled for RSRB networking. Each time the RSRB application finds a router, it does one of the following actions:

- If the router is enabled for RSRB, the discover process stores that router name as an RSRB router in the database, and it polls that router.
- If the router is not enabled for RSRB, the discover process stores that router name as a non-RSRB router in the database, and it does not poll that router.
- If a router cannot be accessed by SNMP, the discover process continues trying to reach that router on every discovery iteration until it can determine whether the router is enabled for RSRB.

There are several ways that the RSRB application can discover the routers in a network. You can provide a list of enabled routers in a special file called a seed file. Or you can let the Maps application get its information from the NMS database.

The discovery methods are described in the following sections:

- Discovering the Network with a Seed File, page 7-19
- Discovering with a Network Management System Database, page 7-21
- Discovering Individual RSRB Routers, page 7-22
- Rediscovering Individual RSRB Routers, page 7-22

Discovering the Network with a Seed File

If your NMS is incapable of providing an accurate list of Cisco routers, or if you want to provide a list of routers that will limit discovery to just a limited set of routers, you can create a seed file for the Maps application.

Seed File Format

Each record in the seed file can be either a comment or a router specification. You can list the routers in any order within the seed file.

Comments

A comment is a single line of text that begins with the pound (#) character, as shown in the following line:

```
# This line is a comment.
```

Router Specifications

A router specification has one of the following formats:

router [*ReadCommunityString*]

or

router:[*ReadCommunityString*]

Use the following conventions for the router specification:

- The delimiter can be a space or a colon (:).
- *router* can be either a host name or the IP address of a router in the network. This is the same label that marks the router on a map.
- *ReadCommunityString* is the read community string for that router. If you do not include this, the default read community string of "public" is used. You can use an asterisk (*) as a place holder for the default read community string, or you can just omit it.

Cross-Application Use

You can use the same seed file for all three Maps applications (DLSw, RSRB, and APPN/SNASw). Although the DLSw application uses a third parameter on each router entry to identify a router as a DLSw key device, that parameter is ignored for the RSRB and APPN/SNASw applications. The following lines are from a sample seed file:

```
# Seed file for CiscoWorks Blue Maps applications
# Next is a non-key router with goldilocks read community string
east.cisco.com goldilocks
# Next is a non-key router with default read community string
172.18.7.47
# Next is a key router with default read community string
west.cisco.com:*:key
# Next is a key router with a read community string
east.cisco.com:readstring:key
```

Note The seed file should not contain any extraneous characters, spaces, or blank lines. Also, remember that the device names and read community strings are case-sensitive.

Using the Seed File for Discovery

To use a seed file for discovery, use the following procedure:

Step 1 Use a text editor to create the seed file. Save the seed file, for example with the name *rsrbseed*.

Step 2 Start RSRB and select **Admin > Discover > Seed File** to display the Seed File Discover window.

Or you can use the CiscoWorks Blue Administration application (**cwbadmin**) described in Chapter 7, "Using the Administration Application."

Step 3 Enter the name of the seed file, verify the correct read community string, and click **Discover**. Discovery takes place while you wait.

After loading the database using the seed file, the application operates normally until a router is taken off line or a new router is configured. If a new router is added to the network, you can perform one of the following tasks:

- Create a new seed file for the new router.
- Add the new routers to the existing seed file and rerun discovery from the seed file. RSRB ignores already discovered routers and discovers just the added routers.
- Add one or more devices directly to the global map, as described in the "Discovering Individual RSRB Routers" section on page 7-22.
- Add one or more devices using the Administration application.

Discovering with a Network Management System Database

The NMS maintains a database which includes all SNMP-managed routers in your network. You can use that database to provide the Maps application with the information it needs to discover the routers in the network.

Discovering the Network Manually

To have the RSRB application discover the network from the NMS database manually, select **Admin > Discover > Database** from the Maps application menu bar. The Maps application adds the routers found by the NMS to the database. The Maps application checks the database for new routers, polls their MIBs, and updates the database with the new MIB information.

Discovering the Network Automatically

You can have Maps check the NMS database automatically. This is called automatic discovery mode; you might want to use it if you expect to install or reconfigure routers often. To use automatic discovery mode, use the **cwb start cwbdiscover** command as a UNIX *cron* job (a chronologically started job). Set the *cron* job to run at night or when system and network activity are low.

Discovering Individual RSRB Routers

If you want to add only one or several routers to your network, you can discover each router individually by using the following procedure:

Step 1 Select **Edit > Add Device(s)** from the menu bar.

Step 2 When prompted, enter the router's device name and its read community string.

Step 3 Click **OK**. The Maps application adds the router to the database, polls the router's MIB, and adds the MIB information to the database.

Watch the status area for a message indicating the success or failure of this polling.

Rediscovering Individual RSRB Routers

It is sometimes useful to rediscover an RSRB router, especially if one of the following events occurs:

- A message appears in the status area indicating that the device already exists in the database.
- A router was just configured with RSRB.
- A later version of the Cisco IOS software was installed on the router so that the RSRB MIB is now supported.
- Router interfaces have been reconfigured or IP addresses have changed.

To rediscover individual routers you can select **Edit > Rediscover Device(s)** from the RSRB menu bar.

Discovering APPN/SNASw in the Network

This section describes the APPN/SNASw discovery process and includes the following subsections:

Understanding APPN/SNASw Discovery

The APPN/SNASw application performs several kinds of discovery:

- APPN/SNASw finds IP addresses and maintains a correlation of IP addresses and APPN/SNASw CP names. APPN/SNASw starts with a network management database, or with a seed file, or just IP addresses. For each address, APPN/SNASw finds an APPN/SNASw name and correlates the device's IP address with its APPN/SNASw name in the correlation table.
- APPN discovers APPN/SNASw nodes. As it checks each IP address, APPN/SNASw looks for the APPN MIB to determine whether that device is APPN/SNASw-enabled.
- APPN discovers network topology agents. As it finds APPN/SNASw-enabled devices, APPN/SNASw checks whether each APPN/SNASw network node can be a network topology agent. APPN/SNASw uses the first network topology agent it finds.

APPN identifies nodes using their APPN/SNASw names, which are in the form *NETID.CPNAME*. *NETID* is the network ID; *CPNAME* is the control point name. To query and collect management data from nodes, APPN/SNASw must also know the IP address for each node (because the APPN/SNASw application manages APPN/SNASw nodes using the SNMP protocol).

The process of finding an IP address for each APPN/SNASw node is called discovery. APPN/SNASw starts with the APPN/SNASw CP name for each node. Then it discovers the IP address by prompting you to enter an IP address or device name (and read community string) for each CP name the first time you request a view. The APPN/SNASw application maintains this correlation between IP address and CP name for subsequent sessions.

To avoid being prompted for IP addresses or host names, you can perform a one-time discovery of the *entire* APPN/SNASw network. For APPN/SNASw, this discovery is the process of querying all IP devices in the network to determine whether they are also APPN/SNASw network nodes, and, if so, to get their APPN/SNASw names.

The APPN/SNASw application stores the correlation data in a binary file named */opt/CSCOcb/etc/appnfile*. You should not edit this file, but you can delete it to force the APPN/SNASw application to lose all its correlation data and rediscover the network. You can delete this file to force rediscovery when CP names or IP addresses are changed or reassigned.

Launching Discovery

You can launch the discovery process by selecting **Admin > Discover** item on the menu bar or from an NMS.

Launching Discovery from the Admin Menu

You can launch the discovery process from the Admin menu in two ways:

- You can launch discovery using a seed file. Select **Admin > Discover > Seed File**. In the Seed File Discover window, select the seed file to start discovery.
- You can launch discovery using a database. Select **Admin > Discover > Database**. The application reminds you that the process could take some time to complete. Click **Yes** if you want to continue.

This process discovers all the devices in the seed file or database. After discovery is complete, select **View > Global** to display the global view.

Launching Discovery Using a Network Management System

We recommend that you do not launch the discovery process using an NMS because the NMS selects a topology agent at random. It is better to explicitly select a topology agent or to use a seed file of network nodes from which to select a network topology agent. APPN/SNASw queries the devices from the seed file in the order in which they are listed. You can launch discovery using an NMS to correlate the IP addresses with CP names for the remaining nodes.

Discovering the Network with a Seed File

An APPN/SNASw seed file is a list of IP devices to be queried for a network topology agent. The APPN/SNASw application uses a seed file in the following situations:

- If you request discovery by seed file in the Startup dialog box
- If you request discovery by seed file after selecting **Admin > DiscoverSeed File**

If your NMS cannot be relied upon for an accurate list of Cisco routers, or if you want to provide a special list of routers, you can create a *seed file for the APPN/SNASw* application.

Seed File Format

Each record in the seed file can be a comment or a router specification. You can list the routers in any order within the seed file, but the order of routers in the seed file determines the order in which the routers are discovered to select a network topology agent.

Comments

A comment is a single line of text that begins with the pound (#) character, as follows:

```
# This line is a comment.
```

Router Specifications

A router specification has one of the following formats:

router [*read_community_string*]

or

router:[*read_community_string*]

Use the following conventions for the router specification:

The delimiter can be a space or a colon (:).

router can be either a host name or the IP address of a router in the network.

read_community_string is the read community string for that router. To use the default string (public), you can omit the *read_community_string* or you can use just an asterisk (*) as a place holder for the default read community string. If a read community string is missing for a device, the APPN/SNASw application uses the default read community string specified by the *rdcommstr* parameter in the *cwbinit* file. You can create the APPN/SNASw seed file with a text editor, and then save it as the *appnseed* file. The recommended location for the seed file is *$HOME/.appn/appnseed*.

Cross-Application Use

You can use the same seed file for all three Maps applications (DLSw, RSRB, and APPN/SNASw). Although DLSw has a third parameter on each router entry to identify a router as a key device, that parameter is ignored for the APPN/SNASw and RSRB applications. The following lines are from a sample seed file:

```
# Seed file for CiscoWorks Blue Maps applications
# Next is a non-key router with goldilocks read community string
east.cisco.com goldilocks
# Next is a non-key router with default read community string
172.18.7.47
# Next is a key router with default read community string
west.cisco.com:*:key
# Next is a key router with a read community string
east.cisco.com:readstring:key
```

Note The seed file should not contain any extraneous characters, spaces, or blank lines. Also, remember that the device names and read community strings are case-sensitive.

Using the Seed File for Discovery

To use a seed file to provide the information to the application, use the following procedure:

Step 1 Use a text editor to create the seed file. Save the seed file, for example with the name *appnseed*.

Step 2 Start APPN/SNASw and select **Admin** > **Discover** > **Seed File**. to display the Seed File Discover window.

You can use the CiscoWorks Blue Administration application (**cwb start admin** command) described in Chapter 7, "Using the Administration Application."

Step 3 Enter the name of the seed file, verify the correct read community string, and click **Discover**. Discovery takes place while you wait.

After loading the database using the seed file, the application operates normally until a router is taken off line or a new router is configured. At that time, you can perform one of the following actions:

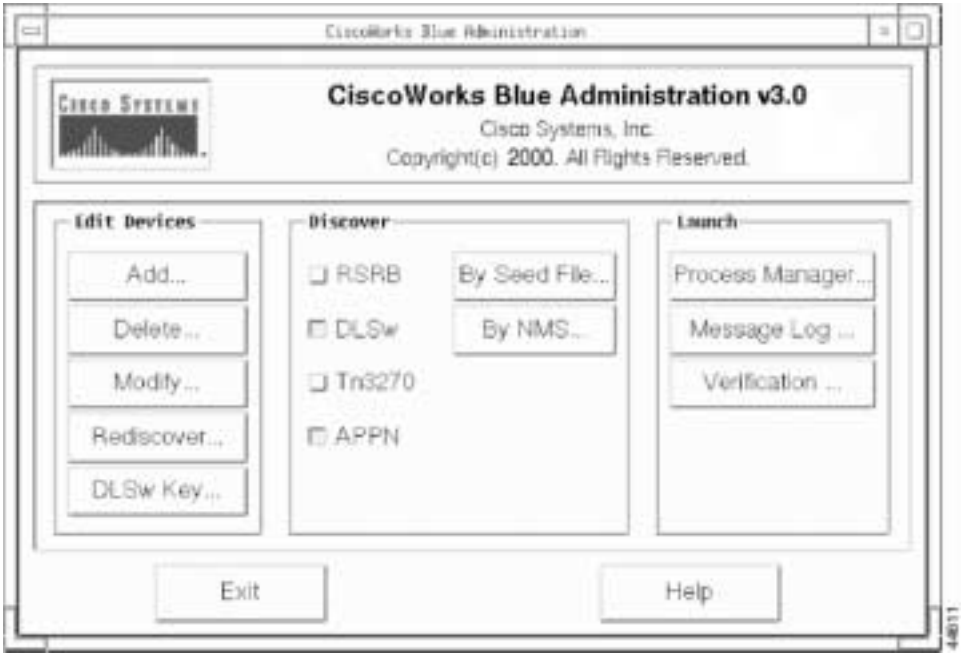
- Create a new seed file to add the new router.
- Add the new routers to the existing seed file and rerun discovery from the seed file. APPN/SNASw ignores already discovered routers and discovers just the added routers.

Discovering Devices for the Database

Use the CiscoWorks Blue Administration application to discover devices for the database. Use the following procedure to discover devices in the database:

Step 1 Display the CiscoWorks Blue Administration window, as shown in Figure 7-3.

Figure 7-3 CiscoWorks Blue Administration Window



Step 2 In the Discover list, select one or more of the following protocol types:

- **RSRB** to discover devices running the RSRB protocol.
- **DLSw** to discover devices running the DLSw protocol.
- **Tn3270** to discover devices running the TN3270 protocol. To use this function, you must have a valid license for the SNA View application.
- **APPN/SNASw** to discover devices running the APPN/SNASw protocol.

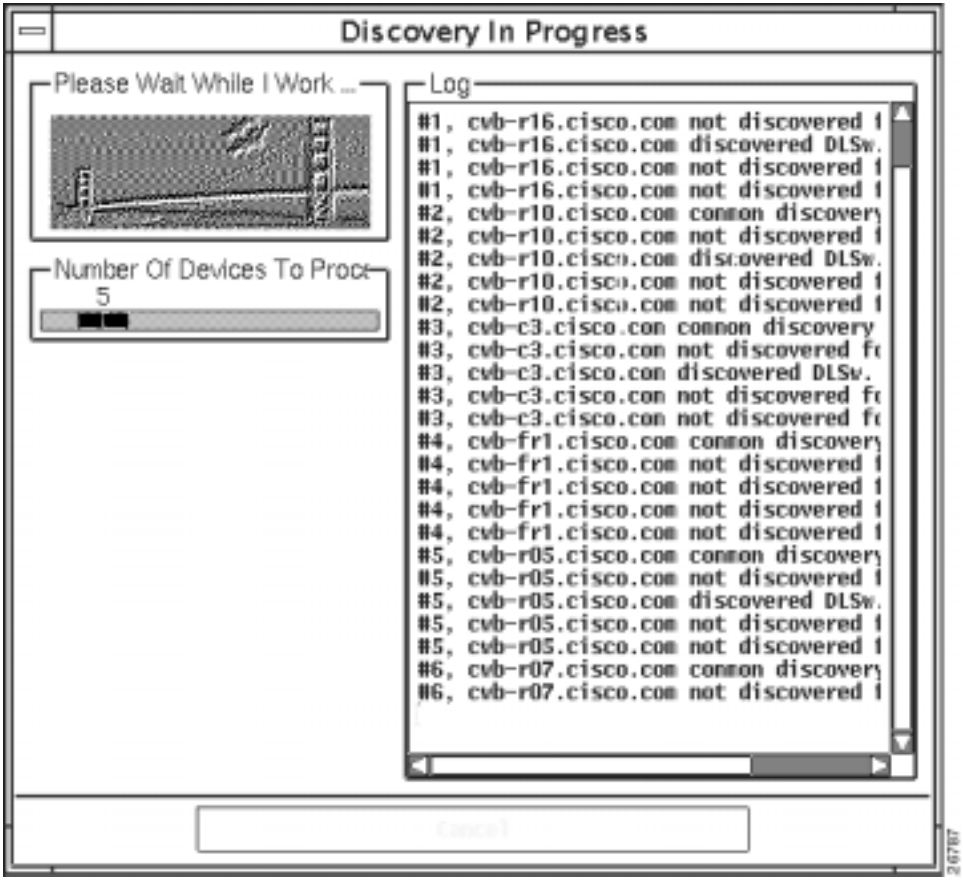
Note After you run discovery for TN3270 or APPN/SNASw, *cwbsnamapsd* is automatically restarted to refresh its cache.

Step 3 Then select a method of discovery:

- Click **By Seed File** to discover the devices using a seed file. You are prompted for the seed file name. When you select this option, the Seed File Discover Window is displayed.
- Click **By NMS** to discover devices using the NMS database. (This option is available only if an NMS was selected during installation.)

The appropriate processes are started to discover and then add enabled devices to the CiscoWorks Blue database during which time the screen displays a work in a Discovery in Progress window. This window is shown in Figure 7-4.

Figure 7-4 Discovery In Progress Window



Seed File Discover Window

Use the Seed File Discover window to select a seed file for discovery.

Fields

The Seed File Discover window has the following fields:

Field	Description
Filter	Allows you to construct a filter rule that controls the paths and files displayed in the Directories and Files fields.
Directories	Displays the directories that meet the filter requirements.
Files	Displays the files that meet the filter requirements.
Selected Seed File	Displays the seed file you selected.
Default Read Community	Displays the default read community string for this seed file. You can change this value.

Buttons

The Seed File Discover window has the following buttons:

Button	Description
Discover	Starts the discover process from the selected seed file.
Filter	Applies the path and file name rule from the Filter field to the Directories and Files fields.

Adding Devices to the Database

You can add one or more devices to the database manually in the following instances:

- You want to add a device that is newly connected to the network.
- You want to add a device to update a set of devices on a map, perhaps because automatic update is disabled, or is set to an infrequent interval and you have not chosen to list target devices in a seed file.

If a Cisco device does not appear on a map or web page, but you know that the device exists in the network, you can add the device using the **Add** button**.**

When you add a device, the application prompts you for the device's host name or IP address and read community string. The application then places the new device in the database.

Use the following procedure to add a device to the database:

Step 1 From the CiscoWorks Blue Administration window, click **Add**. The Add Devices window is displayed, as shown in Figure 7-5.

Figure 7-5 Add Devices Window

Step 2 In the Device name field, enter the host names or IP addresses, separated by spaces, of the devices that you want to add.

Step 3 In the Read Community field, enter the read community string of the device that you want to add.

Step 4 Click **OK**. The new device is added to the database.

After you add new devices, the DLSw poller and *cwbsnamapsd* are automatically restarted to update the following:

- The database with circuit information used in SNA correlation
- The *cwbsnamapsd* cache with current TN3270 and APPN/SNASw information

Deleting a Device From the Database

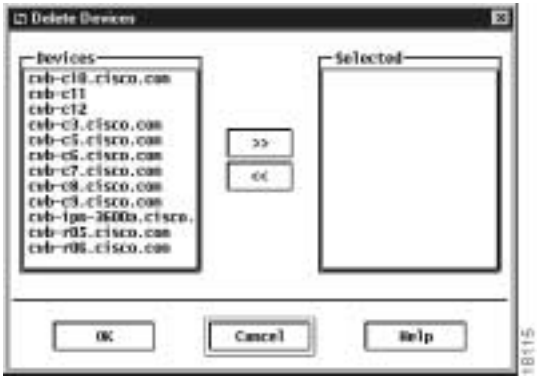
From the CiscoWorks Blue Administration application, you can use the **Delete** button to remove devices from the database. You might want to delete devices for the following reasons:

- The devices might be in the database because you entered incorrect names in a seed file.
- The devices are no longer running any of the managed protocols (DLSw, RSRB, APPN/SNASw, or TN3270).
- You now discover devices from the NMS and have several devices that will never run a managed protocol.
- You have a device that is running a managed protocol but you do not want to manage (poll) that device.
- You want to speed up the discovery process by deleting devices that are not running any of the managed protocols (the discovery process always tries to rediscover devices that are in the database, but not running the selected protocol).

Use the following procedure to delete devices from the database:

Step 1 From the CiscoWorks Blue Administration window, click **Delete**. The Delete Devices window is displayed, as shown in Figure 7-6.

Figure 7-6 Delete Devices Window



Step 2 The Devices list all the devices (routers) in the database. Select all the devices you want to delete.

Step 3 Click the >> button to move the selected devices into the Selected list.

The Selected list displays the devices to be deleted. Use the >> and << buttons to move devices between the Devices list and the Selected list.

If you inadvertently move devices to the Selected list which you do not want to delete, select those devices and click the << button to move them back to the Devices list.

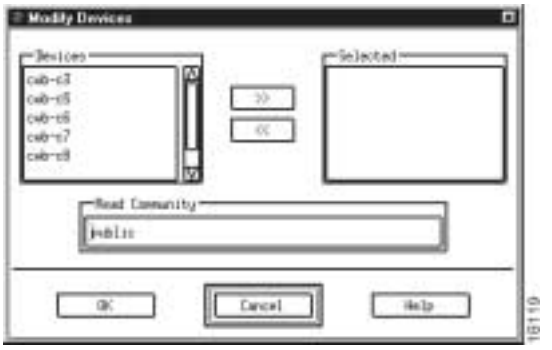
Step 4 Click **OK** to delete the selected devices. The selected devices are deleted from the database.

Modifying a Device in the Database

Change the read community string for one or more devices using the following procedure:

Step 1 From the CiscoWorks Blue Administration window, select **Modify**. The Modify Devices window is displayed and is shown in Figure 7-7.

Figure 7-7 Modify Devices Window



Step 2 The Devices list box displays the devices currently in the database. Select all the devices you want to modify.

Step 3 Click the >> button to move the selected devices into the Selected list. The selected list box displays the devices to be modified. Use the >> and << buttons to move devices between the Devices list and the Selected list.

If you inadvertently move devices which you do not want modified to the Selected list, select those devices and click the << button to move them back to the Devices list.

Step 4 The Read Community string specifies the new read community string for the selected devices. Enter a new read community string to be applied to all the selected devices.

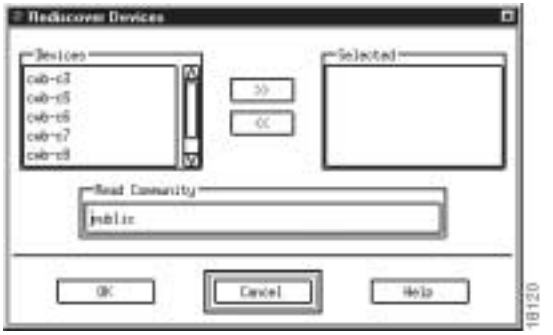
Step 5 Click **OK** to change the read community string for the selected devices. The read community string is changed in the CiscoWorks Blue database (not in the router itself) for the selected devices.

Rediscovering a Device

You may want the discovery process to rediscover a device if that device is now running different protocols; or you may want to update the database information about that device but do not want to wait until the next polling interval. Use the following procedure to rediscover a device:

Step 1 From the CiscoWorks Blue Administration window, select **Rediscover**. The Rediscover Devices window is displayed, as shown in Figure 7-8.

Figure 7-8 Rediscover Devices Window



Step 2 The Devices list displays the devices currently in the database. Select all the devices you want to rediscover.

If you select more than one device by pressing the **Ctrl** or **Shift** key, all selected devices must have the same read community string.

Step 3 Click the >> button to move the selected devices into the Selected list. The Selected list box displays the devices to be rediscovered.

If you inadvertently move devices which you do not want rediscovered, select those devices and click the << button to move them back to the Devices list.

Step 4 The Read Community String field specifies the read community string fort the selected devices. Enter a new read community string to be applied to all the selected devices.

Step 5 Click **OK**. The selected devices are rediscovered.

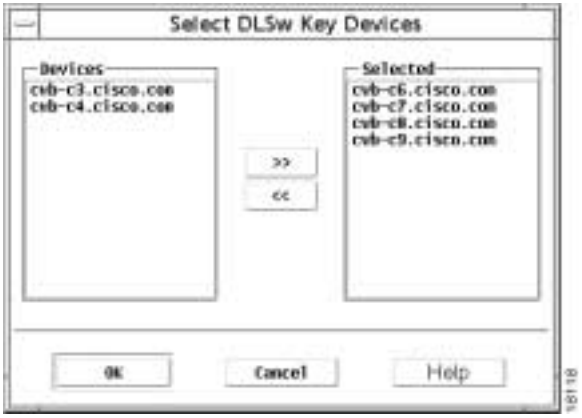
After you rediscover devices, the DLSw poller and *cwbsnamapsd* are automatically restarted to update the database with circuit information used in SNA correlation and to update the *cwbsnamapsd* cache with current TN3270 and APPN/SNASw information.

Specifying DLSw Key Devices

Use the DLSw Key Devices Selection window to designate DLSw key devices from the CiscoWorks Blue database, or to deselect current key devices. You can specify one or more devices as DLSw key devices using the following procedure:

Step 1 From the CiscoWorks Blue Administration window, select **DLSw Key**. The DLSw Key Device Selection window is displayed, as shown in Figure 7-9.

Figure 7-9 Select DLSw Key Devices Window



Step 2 The Devices list displays the DLSw devices that are not key devices. Select all the devices that you want to make key devices.

Step 3 Click the >> button to move the selected devices into the Selected list. The Selected list box displays the DLSw devices that are designated as key devices.

When you click OK, the devices in the Selected list become key devices.

If you inadvertently move devices to the Selected list which you do not want designated as key devices, select those devices and click the << button to move them back to the Devices list.

Step 4 Click **OK**. The devices in the Selected list become DLSw key devices. The devices in the Devices list remain unchanged.

After you add key devices, the DLSw poller is automatically restarted, updating the database with circuit information used in SNA correlation.

Launching the Process Manager Client

You can launch the Process Manager client from the Administration window. From the CiscoWorks Blue Administration window, click **Process Manager**. The Process Manager client application starts and the Process Manager window is displayed.

For information about using the Process Manager, see Chapter 5, “Using the Process Manager.”

Launching the Message Log Client

You can launch the Message Log client from the Administration window. From the CiscoWorks Blue Administration window, click **Message Log**. The Message Log client window is displayed.

For information about using the Message Log viewer, see Chapter 6, “Using the Message Log Viewer.”

Launching the Installation Verification Web Page

You can launch the Installation Verification web page from the Administration window. From the CiscoWorks Blue Administration window, click **Verification**. The web browser is started, which displays the Verification web page. The Verification web page verifies the protocols you configured during installation, checks the *cwbinit* configuration file, and checks the CiscoWorks Blue databas

Starting the User Applications

This chapter provides information on starting the DLSw, RSRB, and APPN/SNASw Motif applications, discovering network devices, using the *cwbinit* preferences file, and starting the CiscoWorks Blue web server for those using UNIX workstations.

This chapter contains the following main sections:

For information on discovery protocols in a network, see Chapter 7, “Using the Administration Application.”

Starting DLSw

This section describes how to start the DLSw application. You can start the DLSw application from the workstation system prompt or from a network management system (NMS), such as NetView for AIX.

Before you start the DLSw application, you should identify at least one or two routers as key devices. If you do not identify key routers in the seed file, the DLSw application cannot display its key devices view and it prompts you to either designate key devices or select another view of the network. You can designate key devices in one of the following ways:

- You can designate key routers using the Administration application, as described in Chapter 7, “Using the Administration Application.”
- You can designate key routers in a seed file, as described in the “Define Key Devices” section on page 2-18.

Verifying the Network Management System

The term network management system (NMS) refers to NetView for AIX, HP OpenView, or Sun Net Manager on the network management workstation.

You can provide network information to DLSw in two ways:

- You can use the database maintained by an NMS.
- You can list all the network devices in a seed file.

If you do not have an NMS, or if the NMS is not up-to-date, or if the NMS database is so large that you do not want a map application to query every device listed, you can create a seed file. A seed file is a text file that lists the routers, and their read community strings, that you want recognized by a specific Maps application. Supply this seed file to the Maps application for each protocol using the procedure in the “Discovering the Network” section on page 7-8.

If you are using an NMS database, verify that the NMS has current data to share with Maps applications before you start DLSw. Even if the NMS is not running at this time, verify that it has been run recently in automanage mode. Also, make sure you ran the discovery process at least once since the last installation of new routers, or reconfiguration of existing routers. If you want to discover new routers as they come online, the NMS must be running in automanage mode continually.

The collection of information and graphical representation of DLSw devices and peer states in the network is usually automatic. You can see a representation of a complete DLSw network, or a narrowed perspective of the DLSw network, including Token Rings, routers, peer statistics, circuit lists and links.

Starting DLSw from a Network Management System

You can start the DLSw application from an NMS, such as NetView for AIX. To start DLSw from an NMS:

- On SunNet Manager, select **Tools > CWB-DLSW** from the menu bar.

- On HP-OV and NetView for AIX, select **CWBlue** > **DLSW** from the menu bar.

Starting DLSw from a System Prompt

You can start DLSw from any valid user account. The installation process establishes a sample default user account named cwblue. The user cwblue does not have a starting password. You can either assign a password to cwblue or log in as root and change to cwblue.

To start the DLSw application from a UNIX workstation system prompt, use the **cwb start dlsw** command, which defines the environment variables, starts the DLSw monitor and poller daemons, and then calls the **dlsw** executable. Enter the following commands:

cd /opt/CSCOcb/bin

./cwb start dlsw

Starting DLSw from a Remote Workstation

You can log in to a remote UNIX host from your own local UNIX workstation, export the remote host display to your local workstation, and then run the application from the remote host. To start the remote host's DLSw application from your local workstation, use the following procedure:

Step 1 At your local UNIX workstation, enter the following command:

xhost +

Step 2 Log in to the remote UNIX host.

Step 3 Set your DISPLAY environment variable to export the display from the remote host to your local workstation. Depending on which shell you are using, use one of the following commands.

- From the K shell (ksh):

export DISPLAY=*IP_address***:0.0**

- From the C shell (csh) or TC shell (tcsh):

  setenv DISPLAY *IP_address***:0.0**

Step 4 To start DLSw, enter the following commands:

cd /opt/CSCOcb/bin

./cwb start dlsw

Starting the Monitor and Poller Daemons

When you start DLSw, the **cwb start dlsw** command uses the **runprocess** script to start the monitor and poller daemons. The monitor and poller daemons monitor the changes in the network, update the database accordingly, and notify the DLSw application when network changes occur. When you exit the DLSw application, all daemons continue to run to maintain the database. If you want to stop them, use the Process Manager, as described in Chapter 5, "Using the Process Manager."

DLSw Initial Startup Sequence

This section describes what happens when you start DLSw for the first time (or when you select **View > Key Devices** from the menu bar).

When it first starts, DLSw tries to display a special view called the key devices view. The key devices view displays the routers that you designated as key devices.

If no devices are specified as key routers, the key devices view is empty. DLSw determines whether there are any routers enabled for DLSw in the database. Based on its finds DLSw-enabled routers in the database, DLSw proceeds as described in the following sections:

- No DLSw Routers in the Database, page 8-5
- DLSw Routers in the Database, page 8-5

No DLSw Routers in the Database

If the key devices view is empty and there are no DLSw routers in the database, then discovery was not done. DLSw displays the following message:

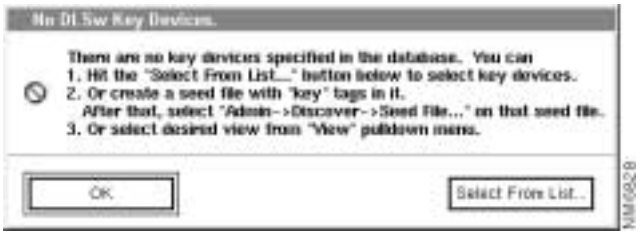
```
Key devices discovery needs to be performed.
Please create a seed file with "key" tags in it.
After that, select Admin->Discover->Seed File.. on that seed file.

OK?
```

Select **Admin** > **Discover** > **Database** or **Admin** > **Discover** > **Seedfile** to discover the network. Now retry the key devices view. If the key devices view is still empty, go to the "DLSw Routers in the Database" section on page 8-5.

DLSw Routers in the Database

If the key devices view is empty, but DLSw routers exist in the database, then discovery was done but no key routers were designated. DLSw displays the message window, as shown in Figure 8-1.

Figure 8-1 No DLSw Key Devices Window



You have the following choices:

- Click **Select From List** in the message window to select key routers from a displayed list of routers.
- Click **OK** to close the window, then select **View > Global** or **View > Focus** from the menu bar to display a global view or a focus view. (At some later time, you should designate at least one key router, as described in the "Define Key Devices" section on page 2-18.)
- Click **OK** to close the window., then use a text editor to create a new seed file with designated key devices. For information about how to designate key devices, see the "Define Key Devices" section on page 2-18. Now select **Admin > Discover > Seed File** from the menu bar to discover the network and refresh the view.

Note If you select **View > Focus** or **View > Global**, and then select **Admin > Discover > Seed File**, the DLSw application refreshes the current focus view or global view. It does not change to the key devices view.

Using the cwbinit Preferences File

The *cwbinit* file contains a set of startup options and variables with which the DLSw application starts. However, if you start DLSw with command-line options, the command-line options override the options set in the *cwbinit* file. These DLSw parameters in the *cwbinit* file are used only by the DLSw poller when it starts. If you change the *cwbinit* file while the poller is running, you must reset the poller to enable the changes in *cwbinit*.

To reset the poller, use the Process Manager or enter the following commands from the command prompt:

/opt/CSCOcb/bin/cwb stop cwbdlswpollerd

/opt/CSCOcb/bin/cwb start cwbdlswpollerd

For each variable that you set in *cwbinit*, ensure that there is a space before and after the equal sign. For example, to set the **eventgen** variable off, enter the following line in *cwbinit*:

eventgen = off

The following *cwbinit* file sample shows only the values that apply to the DLSw application:

```
Cisco Works Blue Maps and SNA View preferences file

# CWBlue applications first check for a user-customized version of
# this file as $HOME/.cwbinit. If the file is not found there, they
# use the installed version at $CWBROOT/etc/cwbinit.

# RULES:
# Keywords must start in column 1.
# There must be a space on each side of the = character.
# Everything on the right of the = character is taken as the value
contents.
# Comments must start with # in column 1 only.
# Comments cannot be included on lines with keywords and values.
# Blank lines are ignored.

# [cwbsnamapsd section deleted]
#
*************************************************************************
# These parameters are only read at startup time by the DLSw poller
# (cwbdlswpollerd) and APPN/SNASw applications (cwbsnamapsd and
APPN/SNASw).

# ************************************************
# *** Global parameters used by both DLSw and APPN/SNASw ***
# ************************************************

# This parameter controls how often cwbdlswpollerd and cwbsnamapsd
# will check to see if another process has requested that it recycle
# itself. Other processes make this request after APPN/SNASw, TN3270,
and/or # DLSW discovery/rediscovery and after DLSW key routers are
assigned. # The DLSw poller and cwbsnamapsd processes periodically
```

```
check to see # if a restart request has been made. The value supplied
is in
# seconds.

processRestartInterval = 30
# to turn off event generation set eventgen = off.
# valid values : on/off. default value : on.
eventgen = on

# to turn on device state change event generation set eventgen_device
# = on.
# valid values : on/off. default value : off.
eventgen_device = off

# ***********************
# *** DLSw parameters ***
# ***********************
# These parameters are used by the DLSw poller. If the poller is
# already running, it must be stopped and restarted from the process
# manager, or from the command line as follows:
# $CWBROOT/etc/runprocess cwbdlswpollerd -f

# *** DLSw event generation parameters ***

# to turn off dlsw peer event generation set eventgen_dlswpeercxn =
# off. valid values : on/off. default value : on.
eventgen_dlswpeercxn = on

# to turn on dlsw circuit event generation set eventgen_dlswcircuit =
# on. valid values : on/off. default value : off.
eventgen_dlswcircuit = off

# *** DLSw polling parameters ***

# to set key routers polling timer set keyPeerSleepTime = <number of
# seconds. valid range of values : 0 to 65535 seconds. default value :
# 600 seconds.
keyPeerSleepTime = 600

# to turn on slow polling of non-key dlsw peer routers set
# pollNonKeyPeer = on. valid values : on/off. default value : on.
# pollNonKeyPeer = on

# to set slow polling timer set nonKeyPeerSleepTime = <number of
# seconds. valid range of values : 0 to 65535 seconds. default value :
# 600 seconds.
nonKeyPeerSleepTime = 600
```

```
# to turn on circuit polling of dlsw key routers set pollKeyCircuit =
# on. valid values : on/off. default value : on.
pollKeyCircuit = on

# to set circuit polling timer set keyCircuitPollSleepTime = <number
# of seconds. valid range of values : 0 to 65535 seconds. default
# value : 1200 seconds.
keyCircuitPollSleepTime = 1200

# to set number of threads for polling key router peer connections set
# numKeyPeerPollThreads = <number>.
# valid range of values : 1 to 10. default value : 5.
numKeyPeerPollThreads = 5

# to set number of threads for polling non-key router peer connections
# set numNonKeyPeerPollThreads = <number>.
# valid range of values : 1 to 10. default value : 1.
numNonKeyPeerPollThreads = 1

# to set number of threads for polling key router circuits
# set numKeyCircuitPollThreads = <number>.
# valid range of values : 1 to 10. default value : 1.
numKeyCircuitPollThreads = 1

# to set sleep time for directed poll set
# directedPollSleepTime = <number of seconds>.
# valid range of values : 0 to 65535 seconds. default value : 0.
directedPollSleepTime = 0

# to set action to take when peers are down set
# peerDownAction = <executable Name>
# valid values : /path/executableName
# passed parameters : Local-Ip-Address Remote-Ip-Address
# peerDownAction =

# to set action to take when circuits are down set
# circuitDownAction = <executable Name>
# valid values : /path/executableName
# passed parameters : MacAddress1 SAP1 MacAddress2 SAP2
#circuitDownAction =

# to poll additional devices for dlsw
# peer connections at the rate of key-peer-poll and
# circuits at the rate of circuit-poll
# additionalPollRouterList = <router_name separated by ', '>
# valid values : router1.name.com, router2.name.com
#additionalPollRouterList =
.[APPN parameters Deleted]
```

Using cwbinit to Configure Event Notification

You can configure the DLSw application to generate event notifications (trap messages) when specific network events occur. These events can include device state changes, peer connection state changes, and changes to the status of a circuit. When a specified network event occurs, DLSw sends an event notification to the UNIX NMS.

Use the following event values in the *cwbinit* file to specify whether to send event notifications and to configure which events will cause trap messages to be sent.

- Use the **eventgen** value to set event notification on and off. If you set **eventgen = on**, event notification is enabled. The default setting is **on**.
- Use the **eventgen_device** value to set device-state event notification on and off. If you set **eventgen_device = on**, an event notification is generated whenever a device state changes. The default setting is **off**.
- Use the **eventgen_dlswpeercxn** value to set peer-connection event notification on and off. If you set **eventgen_dlswpeercxn = on**, an event notification is generated whenever a DLSw peer connection state changes. The default setting is **on**.
- Use the **eventgen_dlswcircuit** value to set circuit-state event notification on and off. If you set **eventgen_dlswcircuit = on**, an event notification is generated whenever a DLSw circuit state changes. The default setting is **on**.

After you configure the event notification options, DLSw will send trap messages to the NMS at your UNIX workstation. Chapter 10, “Event Notification Messages,” describes the trap messages sent by the Maps applications.

Using cwbinit to Configure Process Restarting Intervals

Use the **processRestartInterval** value to control how often, in seconds, the **cwbdlswpollerd** and **cwbsnamapsd** processes check to see whether some other process has requested that it recycle itself. Other CiscoWorks Blue processes make this request after APPN/SNASw, TN3270, and DLSW discovery and rediscovery, and after DLSW key routers are assigned. The DLSw poller and **cwbsnamapsd** processes periodically check to see if a restart request has been made. The default value is 30 seconds.

Using cwbinit to Configure Polling Intervals

You can configure how the DLSw application polls routers for peer connection information and for circuit information. You can select from the following polling methods:

- Key-Peer polling polls just key routers for peer connection information. To control the Key-Peer polling rate use the **KeyPeerSleepTime** option of the **cwb start cwbdlswpollerd** command, as described in Appendix D, "CiscoWorks Blue Commands and Processes."
- Non-Key-Peer polling polls just the non-key routers for peer connection information. To control the Non-Key-Peer polling rate, use the **nonKeyPeerSleepTime** value.
- Key-Circuit polling polls just the key routers for circuit information. To control the Key-Circuit-Peer polling rate, use the **keyCircuitPollSleepTime** value. To control the Key-Router polling rate, use the **keyPeerSleepTime** value:

If you make no changes, the DLSw polling daemon uses all three polling methods: it polls key routers and non-key routers for peer connection information, and it polls key routers for circuit information. You can change these selections using the following polling values in the *cwbinit* file.

- Use the **pollNonKeyPeer** value to set non-key-peer polling on and off. If you set it on, non-key routers are polled for peer connection information. The default value is on.
- Use the **nonKeyPeerSleepTime** value to specify the sleep time for non-key-peer polling. This sleep-time value determines how many seconds the poller daemon waits after polling all the non-key routers before it starts polling them again. The valid range is from 0 to 65535 seconds. The default value is 600 seconds.
- Use the **pollKeyCircuit** value to set key-circuit polling on and off. If you set it on, circuit polling is enabled; key routers are polled for circuit information. The default value is on.

- Use the **keyCircuitPollSleepTime** value to set the sleep time value for key-circuit polling key routers for their circuits. This sleep-time value determines how many seconds the poller daemon waits after polling all the key routers before it starts polling them again. The valid range is from 0 to 65535 seconds. The default value is 1200 seconds. You can override the **keyCircuitPollSleepTime** value using the **-C PollingSleepTime** value on the *cwbdlswpollerd* daemon, as described in Appendix D, "CiscoWorks Blue Commands and Processes."
- Use the **keyPeerSleepTime** value to set the sleep time value for polling key routers for the peer tables to keep the maps current. This sleep-time value determines how many seconds the poller daemon waits after polling all the key routers before it starts polling them again. The valid range is from 0 to 65535 seconds. The default value is 600 seconds. You can override the **keyPeerSleepTime** value using the **PollingSleepTime** value on the *cwbdlswpollerd* daemon, as described in Appendix D, "CiscoWorks Blue Commands and Processes."
- Use the **numKeyPeerPollThreads** value to define the number of threads that can be used for key-peer polling. You can set this value to a number in the range 1 to 10. The default value is 5 threads. If you increase this value, DLSw increases the number of routers that are polled concurrently, but uses more network bandwidth.
- Use the **numNonKeyPeerPollThreads** value to define the number of threads that can be used for polling non-key routers for peer connection information. You can set this value to a number in the range 1 to 10. The default value is 1 thread.
- Use the **numKeyCircuitPollThreads** value to define the number of threads that can be used for circuit polling. You can set this value to a number in the range 1 to 10. The default value is 1 thread.

- Use the **directedPollSleepTime** value to set a sleep time for directed polling. Directed polls go to a non-key router when a key router reports a lost connection. This verifies the status of the remote router. When you define a number of threads for key-router polling, non-key-router polling, and circuit polling, the poller daemon adds one extra thread for additional polling of remote routers. This sleep-time value determines how many seconds this extra thread waits after polling is complete before it starts polling again. The valid range is from 0 to 65535 seconds. The default value is 0 seconds. You can increase this setting to slow down the rate of directed polling of remote routers.
- Use the **additionalPollRouterList** value to add specific non-key routers to the key-peer polling list. This entry is terminated with a carriage return; the entire entry must be no more than 100 characters. For example, to add non-key routers named routera.domain.com and routerb.domain.com to the key-router polling list (but not to the key devices view), you would add this line to the *cwbinit* file:

  ```
  additionalPollRouterList = routera.domain.com,routerb.domain.com
  ```

Using Event Generation Exits

The **peerDownAction** and **circuitDownAction** event generation exits let you create your own exit routines to handle situations in which key routers do not respond to polling for peer connection information or for circuit information.

Use the **peerDownAction** value to define a program to be run when routers do not respond to polling for peer connection information. Replace the string *executableName* with the name of your application. The poller daemon calls your application with the following command format:

```
user_application local_IP_address remote_IP_address
```

Where:

user_application is the name of the program that you supply.

local_IP_address is the IP address of the local peer.

remote_IP_address is the IP address of the remote peer.

Use the **circuitDownAction** value to define a program to run when key routers do not respond to polling for circuit information. Replace the string *executableName* with the name of your application. The poller daemon calls your application with the following command format:

```
user_application MACAddress1 SAP1 MACAddress2 SAP2
```

Where:

user_application is the name of the program that you supply.

MACAddress1 is the MAC address of the local peer.

SAP1 is the SAP of the local peer.

MACAddress2 is the IP address of the remote peer.

SAP2 is the SAP of the remote peer.

When your exit routine is invoked by one of these exits, you have the followig options:

- You can write a troubleshooting application to further investigate the problem and do some error correction at the router.
- You can send the information passed by the exit to a network administrator for further action.

Starting RSRB

This section describes how to start the RSRB application. You can start the RSRB application either from the workstation system prompt or from a NMS, such as NetView for AIX.

Verifying the Network Management System

The term network management system (NMS) refers to NetView for AIX, HP OpenView, or Sun Net Manager on the network management workstation.

You can provide network information to RSRB in two ways. You can use the database maintained by an NMS, such as NetView for AIX, HP OpenView, or Sun Net Manager, or you can list all the network devices in a seed file. If you do not have an NMS, or if the NMS is not up-to-date and cannot be updated, or if you know the NMS database is so large that you do not want a map application to spend the time querying every device listed there, you can create a seed file. A seed file is a text file that lists the routers, and their read community strings, that you want to be recognized by a specific Maps application. Supply this seed file to the Maps application for each protocol using the procedure in the “Discovering the Network” section on page 7-8.

If you are using an NMS database, verify that the NMS has current data to share with Maps applications before you start RSRB. Even if the NMS is not running at this time, verify that it has been run recently in automanage mode or that you have run the discovery process at least once since the last installation of new routers or reconfiguration of existing routers. If you want to discover new routers dynamically as they come online, the NMS must be running in automanage mode continually.

The collection of information and graphical representation of RSRB devices and peer states in the network is usually automatic. You can see a representation of a complete RSRB network or a narrowed perspective of the RSRB network, including virtual rings, physical rings, routers, and links.

Starting the RSRB Application from a Network Management System

You can start the RSRB application from an NMS such as NetView for AIX. To start RSRB from an NMS:

- On SunNet Manager select **Tools > CWB-RSRB** from the menu bar.
- On HP-OV and NetView for AIX select **CWBlue > RSRB** from the menu bar.

Starting RSRB from a System Prompt

You can start RSRB from any valid user account. The installation process establishes a sample default user account named cwblue. The user cwblue does not have a starting password. You can either assign a password to cwblue or log in as root and change to cwblue.

To start the RSRB application from a UNIX workstation system prompt, enter the command shown below:

cd /opt/CSCOcb/bin

./cwb start rsrb

Starting RSRB from a Remote Workstation

You can log in to a remote UNIX host from your own local UNIX workstation, export the remote host display to your local workstation, and then run the application from the remote host. To start the remote host's RSRB application from your local workstation, use the following procedure:

Step 1 At your local UNIX workstation, enter the following command:

xhost +

Step 2 Log in to the remote UNIX host.

Step 3 Set your DISPLAY environment variable to export the display from the remote host to your local workstation. Depending on which shell you are using, use one of the following commands:

- From the K shell (ksh):

  export DISPLAY=*IP_address***:0.0**

- From the C shell (csh) or TC shell (tcsh):

  setenv DISPLAY *IP_address***:0.0**

- To start RSRB, enter the following commands:

  cd /opt/CSCOcb/bin

  ./cwb start rsrb

Starting the Monitor and Poller Daemons

When you start RSRB, the **cwb start rsrb** command script automatically starts the monitor and poller daemons that monitor the changes in the network and update the database accordingly. When you exit the RSRB application, all daemons continue to run to maintain the database. If you want to stop them use the Process Manager, as described in Chapter 5, "Using the Process Manager."

Starting APPN/SNASw

You can start the APPN/SNASw application from the workstation system prompt, from a remote workstation, or from an NMS, such as NetView for AIX.

Starting APPN/SNASw from the System Prompt

You can start APPN/SNASw from any valid user account. The installation process establishes a sample default user account named cwblue. The user cwblue does not have a starting password. You can either assign a password to cwblue or log in as root and change to cwblue.

To start the APPN/SNASw Maps application from a system prompt, enter the following commands:

cd /opt/CSCOcb/bin

./cwb start appn [**-f** *devicename* [**-r** *read_community_string*]] [**-v**] [**-h**]

Where:

-f *devicename* specifies the host name or IP address of an APPN node to be used as the network topology agent.

Note For SNASw networks, do not specify the **-f** parameter.

-r *read_community_string* specifies *the read community string for the router specified by devicename.* APPN/SNASw uses the *read_community_string* value when communicating with an APPN/SNASW node. If you do not enter a *read community string*, the APPN/SNASW application uses the default *read community string* specified in the *cwbinit* file or, if there is not one there, the default string “public.”

Note For SNASw networks, do not specify the **-r** parameter.

-v displays version information.

-h displays online help.

Starting APPN/SNASw from a Remote Workstation

You can log in to a remote UNIX host from your own local UNIX workstation, export the remote host display to your local workstation, and then run the application from the remote host.

To start the remote host's APPN/SNASW application from your local workstation, use the following procedure:

Step 1 At your local UNIX workstation, enter the following command:

xhost +

Step 2 Log in to the remote UNIX host.

Step 3 Set your DISPLAY environment variable to export the display from the remote host to your local workstation. Depending on which shell you are using, use one of the following commands:

- From the K shell (ksh):

  export DISPLAY=*IP_address***:0.0**

- From the C shell (csh) or TC shell (tcsh):

  setenv DISPLAY *IP_address***:0.0**

Step 4 To start APPN/SNASW, enter the following commands:

cd /opt/CSCOcb/bin

./cwb start appn [**-f** *devicename* [**-r** *read_community_string*]] [**-v**] [**-h**]

Where:

-f *devicename* specifies the host name or IP address of an APPN/SNASw node to be used as the network topology agent. APPN/SNASw displays a global view at startup.

-r *read_community_string* specifies *the read community string for the router specified by devicename.* APPN/SNASw uses the *read_community_string* value when communicating with APPN/SNASw nodes. If you do not enter this value, the program uses the default *read community string* "public," unless another default string is specified in the *cwbinit* file.

-v displays version information.

-h displays online help.

Starting APPN/SNASw from a Network Management System

You can start APPN/SNASw from an NMS like NetView for AIX. To start APPN/SNASw from an NMS:

- On SunNet Manager select **Tools > CWB-APPN** from the menu bar.
- On HP-OV and NetView for AIX select **CWBlue > APPN/SNASw** from the menu bar.

Starting APPN/SNASw with No Options

If you start APPN/SNASw from NetView, or if you do not enter any options with the **cwb start appn** command, the APPN/SNASw application looks in its preferences file, */opt/CSCOcb/etc/cwbinit*, for the control point (CP) name, or for an IP address or device name (and read community string) of a network topology agent. If a network topology agent is not specified in the *cwbinit* file, APPN/SNASw polls all discovered APPN/SNASw routers and does not use a network topology agent.

Note When you first start APPN/SNASw, select **Admin > Discover** to discover the APPN/SNASw routers in your network.

Selecting a Network Topology Agent

This section describes how you can select a network topology agent, which is an APPN network node that provides information about the backbone APPN/SNASw network. A network topology agent is optional.

Because a mechanism exists to poll only for updates, specifying a network topology agent makes for more efficient monitoring of the backbone APPN/SNASw topology.

Note An SNASw branch network node cannot serve as a network topology agent.

To select a network topology agent, specify it in the *cwbinit* file. For more information, see the "Using cwbinit to Specify a Network Topology Agent" section on page 8-24.

Using the cwbinit Preferences File

The *cwbinit* file contains a set of startup options and variables for the APPN/SNASw application. However, if you start APPN/SNASw with command-line options, the command-line options override the options set in the *cwbinit* file.

These APPN/SNASw parameters in the *cwbinit* file are used only when you issue the **cwb start appn** command. If you change the *cwbinit* file while the APPN/SNASw application is running, you must stop and restart the APPN/SNASw application to activate the changes in *cwbinit*.

To reset the APPN/SNASw application, select **File > Exit Program** from the APPN/SNASw menu bar. Then restart the APPN/SNASw application using the following command:

cd /opt/CSCOcb/bin

./cwb start appn

For each variable you set in *cwbinit*, ensure that there is a space before and after the equal sign. For example, to turn off the **eventgen** variable, you would enter the following line in *cwbinit*:

```
eventgen = off
```

Each APPN/SNASw user can have a private *cwbinit* file. If the APPN/SNASw application cannot find the file *$HOME/.cwbinit*, it uses the file */opt/CSCOcb/etc/cwbinit*. You might want to use a set of private cwbinit files to monitor different APPN/SNASw networks from different user IDs.

The following shows a sample *cwbinit* file stored during installation of CiscoWorks Blue Maps:

```
# Cisco Works Blue Maps and SNA View preferences file

# CWBlue applications first check for a user-customized version of
# this file as $HOME/.cwbinit. If the file is not found there, they
# use the installed version at $CWBROOT/etc/cwbinit.

# RULES:
# Keywords must start in column 1.
# There must be a space on each side of the = character.
# Everything on the right of the = character is taken as the value
contents.
# Comments must start with # in column 1 only.
# Comments cannot be included on lines with keywords and values.
# Blank lines are ignored.

# [cwbsnamapsd section deleted]

#
**********************************************************************
# These parameters are only read at startup time by the DLSw poller
# (cwbdlswpollerd) and APPN/SNASw applications (cwbsnamapsd and
APPN/SNASw).

# ************************************************
# *** Global parameters used by both DLSw and APPN/SNASw ***
# ************************************************

# This parameter controls how often cwbdlswpollerd and cwbsnamapsd
# will check to see if another process has requested that it recycle
# itself.
# Other processes make this request after APPN/SNASw, TN3270, and/or
DLSW
# discovery/rediscovery and after DLSW key routers are assigned. The
# DLSw poller and cwbsnamapsd processes periodically check to see if a
# restart request has been made. The value supplied is in seconds.

processRestartInterval = 30
# to turn off event generation set eventgen = off.
# valid values : on/off. default value : on.
eventgen = on

# to turn on device state change event generation set eventgen_device
= on.
# valid values : on/off. default value : off.
eventgen_device = off
.
. [DLSw parameters Removed]
# **********************
```

```
# *** APPN/SNASw parameters ***
# **********************
# These parameters are used by both appn and cwbsnamapsd. If either
# are already running, they must be stopped and restarted for changes
# to take effect.

# Selection of the network topology agent is done in this order:
# 1) command line parameters, if any;
# 2) parse this config file.
# 3) user will be prompted to run discovery or enter agent information
#
# #3 applies to appn only. No prompt dialog is given in cwbsnamapsd.

# network topology agent ip address or device name (NOT appn cpname)
nettopoagentdevname =

# network topology agent read community string
nettopordcommstr =

# network topology agent APPN control point name (NETID.CPNAME format)
nettopoagentcpname =

# backup network topology agent ip address or device name (NOT APPN
cpname)
backupnettopoagentdevname =

# backup network topology agent read community string
backupnettopordcommstr =
# backup network topology agent APPN control point name (NETID.CPNAME
format)
backupnettopoagentcpname =

# default read community string
rdcommstr = public

# automatic collection of local topology (NONE, NN_ONLY, ALL)
autolocaltopo = ALL

# network topology polling interval, in seconds
nettopopoll = 15

# backup network topology polling interval, in seconds
# (in backup mode only, when primary agent fails, backup uses
nettopopoll)
backupnettopopoll = 600


# local topology polling interval, in seconds
```

```
loctopopoll = 600

# control whether APPN/SNASw polls the DLUR PU table as part of local
topology
# polling. To turn off polling for PUs, set appn_pu_polling = off
appn_pu_polling = on

# control whether APPN/SNASw polls the APPN port table as part of
local topology
# polling. To turn off polling for ports, set appn_port_polling = off
appn_port_polling = on

# control whether APPN/SNASw polls the APPN link table as part of
local topology
# polling. To turn off polling for links, set appn_link_polling = off
appn_link_polling = on

# This option controls TG event generation.
# To turn off TG event generation, set eventgen_tg = off.
# To generate event for existing TGs when an operational state change
# is detected, set eventgen_tg = on.
# To generate events for existing TGs when an operational state change

# is detected and for newly created operational (active) TGs,
# set eventgen_tg = all.
# Exception: No events are generated for TGs created on
# the first poll cycle. This avoids a storm of events during
# process startup.
# valid values: on/off/all
eventgen_tg = on

# to turn off dlur session event generation set eventgen_dlur = off
# valid values : on/off
eventgen_dlur = on

# to turn on port event generation set eventgen_port = on
# valid values : on/off
eventgen_port = off
# to turn on link event generation set eventgen_link = on
# valid values : on/off
eventgen_link = off

# This option controls the CWBlue cache deletion of TGs that are no
# longer reported by local topology agents. A Cisco IOS change was
# made to delete inactive dynamic TGs from the router database.
# To delete TGs that are no longer reported by the agent,
# set this parameter to 'off'.
```

```
# To keep those TGs in the CWBlue cache, set this parameter to 'on'.
If TG
# events are enabled, this will trigger an event if the TG becomes
# operational again.
# valid values:on/off
keep_deleted_tgs = off
```

Using cwbinit to Specify a Network Topology Agent

You can use the *cwbinit* file to specify a network topology agent for APPN in one of the following ways:

Note Do not use this parameter for SNASw routers.

- You can specify the host name or IP address and read community string of a single APPN node from which to collect network topology. Use the **nettopoagentdevname** and **nettopordcommstr** variables in the *cwbinit* file to identify the agent name and read community string.
- You can specify the APPN CP name, in *NETID.CPNAME* format, of a single APPN node from which to collect network topology. Use the **nettopoagentcpname** variable in the *cwbinit* file to identify the CP name.

If you specify a network topology agent in the *cwbinit* file, you can also specify a backup network topology agent in the *cwbinit* file. Specify the backup network topology agent in one of the following ways:

- You can specify the host name (or IP address) and read community string of the backup network topology agent. Use the **backupnettopoagentdevname** and **backupnettopordcommstr** variables in the *cwbinit* file to identify the backup agent name and read community string.
- You can specify the APPN CP name, in *NETID.CPNAME* format, of the backup network topology agent. Use the **backupnettopoagentcpname** variable in the *cwbinit* file to identify the backup agent CP name.

If APPN cannot collect network topology from the agent you identify, it tries again, using the interval specified by the **nettopopoll** variable in the *cwbinit* file.

Using cwbinit to Configure Process Restarting Intervals

Use the **processRestartInterval** value to control how often, in seconds, the **cwbdlswpollerd** and **cwbsnamapsd** processes check to see whether some other process has requested that it recycle itself. Other CiscoWorks Blue processes make this request after APPN/SNASw, TN3270, and DLSW discovery and rediscovery and after DLSW key routers are assigned. The DLSw poller and **cwbsnamapsd** processes periodically check to see if a restart request has been made. The default value is 30 seconds.

Using cwbinit to Set the Frequency of APPN/SNASw Polling

Network topology polling is the periodic collecting of data from the network topology agent. Local topology polling is the periodic collecting of data from each APPN/SNASw node.

Because the overhead of network topology polling is less than the overhead of local topology polling, the APPN/SNASw application performs network topology polling more frequently than local topology polling. To control the polling frequency, use the **nettopopoll**, **loctopopoll**, and **backupnettopopoll** parameters in the *cwbinit* file.

You can use the **appn_pu_polling** parameter to control polling for PU information. If you set **appn_pu_polling = on**, APPN/SNASw polls for PU information at the interval specified by the **loctopopoll** parameter. The **appn_pu_polling** parameter affects polling only; it does not affect the collecting of local topology when you select **Get Local Topology** from a popup menu.

Using cwbinit to Facilitate the Generation of Views

The APPN/SNASw application collects and stores local topology data collected from an APPN/SNASw node. The APPN/SNASw application usually collects local topology data on demand, such as when the generation of a view requires it. To expedite the generation of some views, and to assure the completeness of adjacent-node views, set the **autolocaltopo** parameter to one of the following values:

- ALL automatically polls local topology data from all APPN/SNASw nodes for which SNMP information is already available at the interval specified by the **loctopopoll** parameter in the *cwbinit* file. ALL is the default.

- NN_ONLY automatically polls local topology data only from network nodes (including branch network nodes) for which SNMP information is already available at the interval specified by the **loctopopoll** parameter in the *cwbinit* file.
- NONE does not poll local topology data automatically.

Using cwbinit to Configure Event Notification

You can configure the APPN/SNASw application to generate event notifications (trap messages) when specific network events occur. These network events can include changes to a transmission group's state, changes to a DLUS-DLUR session state, and changes to the status of a node, a port, or a link. When the specified network event occurs, APPN/SNASw sends a trap message to the NMS.

Use the following event values in the *cwbinit* file to specify whether to send event notifications and to specify which events will cause trap messages to be sent:

- Use the **eventgen** value to set event notification on and off. If you set **eventgen = on**, event notification is set on (enabled). If you set **eventgen = off**, all event notification is set off (disabled) regardless of the settings of other parameters.
- Use the **eventgen_device** value to set device-state event notification on and off. If you set **eventgen_device = on**, an event notification is generated whenever a device state changes.
- Use the **eventgen_tg** value to set TG event notification on and off.
  - Set **eventgen_tg=on** to generate an event when an existing TG has a change in operational status.
  - Set **eventgen_tg=off** to not generate events for any TG status changes.
  - Set **eventgen_tg=all** to not generate an event whenever an existing TG has a change in operational status and when a new TG becomes active.

    Events are not generated during the first polling cycle for each agent to prevent events for every active TG from being sent because all TGs will be new to the CiscoWorks Blue cache.
- Use the **eventgen_dlur** value to set DLUR-state event notification on and off. If you set **eventgen_dlur = on**, an event notification is generated whenever a DLUR state changes.

- Use the **eventgen_port** value to set port-state event notification on and off. If you set **eventgen_port = on**, an event notification is generated whenever a port state changes.
- Use the **eventgen_link** value to set link-state event notification on and off. If you set **eventgen_link = on**, an event notification is generated whenever a link state changes.

After you configure the event notification options, APPN/SNASw will send trap messages to the NMS at your UNIX workstation. Chapter 10, "Event Notification Messages," provides a list and descriptions of the trap messages sent by the Maps applications.

Using cwbinit to Specify Whether to Delete Inactive TGs

Use the **keep_deleted_tgs=on** value to keep inactive TGs in the Maps and SNA View cache. The Cisco IOS software deletes inactive dynamic TGs from the router database. If you want to keep those inactive TGs in the Maps and SNA View cache, set the **keep_deleted_tgs=on** option in the *cwbinit* file. If you want to delete those inactive TGs from the Maps and SNA View cache, set the **keep_deleted_tgs=off** option in the *cwbinit* file.

Improving Performance

This chapter provides information on techniques you can use to improve the performance of the CiscoWorks Blue applications.

This chapter includes the following main sections:

Stopping the Monitor Daemon

If you are locked out of Maps views due to continual view updates, try stopping the monitor daemon so that it will not keep trying to update the maps. To stop the monitor daemon, use the Process Manager client or use the **cwb stop cwbmonitord** command. You must now manually refresh the Maps views because they are no longer automatically updated.

Stopping the Poller Daemon While Doing Discovery

Before you select **Administration > Discover** to discover your DLSw or RSRB network, stop the poller daemon using either the **cwb stop cwbrsrbpollerd** or **cwb stop cwbdlswpollerd** command or the Process Manager. When discovery is done, you can restart the poller daemon using the **cwb start cwbrsrbpollerd** or **cwb start cwbdlswpollerd** command or the Process Manager.

Limiting Remote Users

If you are running short of memory at the Maps workstation, you should limit the number of remote Maps users. Each Maps session requires approximately 20 MB of system memory in addition to the memory needed to display each graphical map.

Closing Unused Maps Windows

You should close the Maps windows when you no longer need them open. When several Maps windows are open, any change in a view to any one of the open windows causes all Maps windows to hang until the changing view has been completely refreshed. The delay is especially noticeable when a change occurs in a global view, in which any network change can result in a lengthy update cycle.

Improving DLSw Poller Performance

There are several changes you can make to improve the performance of the DLSw poller. You can customize the number of active threads to improve the bandwidth or the response time, and you can limit the amount of polling in the network.

Improving Bandwidth or Response Time

You can make changes to the DLSw poller's threads and sleep times on UNIX workstations (described in the "Using cwbinit to Configure Polling Intervals" section on page 8-11) that will improve either bandwidth (the amount of network resources consumed by DLSw) or response time (the time it takes the DLSw application to detect a change in the network):

- To decrease the bandwidth, decrease the number of threads, and increase the sleep time.
- To improve response time, increase the number of threads, and decrease the sleep time.

Changing the Number of Threads

You can change the number of threads by changing the values of these **numKeyPeerPollThreads**, **numNonKeyPeerPollThreads**, and **numKeyCircuitPollThreads** variables in the *cwbinit* file.

Changing the Sleep Times

You can change the sleep times by changing the values of the **keyCircuitPollSleepTime**, **nonKeyPeerPollSleepTime**, and **directedPollSleepTime** variables in the *cwbinit* file.

Limiting Polling

You can make changes that will limit the amount of polling done by the DLSw application.

- If you do not need SNA-correlation with DLSw circuits, you can stop DLSw circuit polling. To stop DLSw circuit polling, set **pollKeyCircuit = off** in the *cwbinit* file.
- If you do not want to poll the remote routers, set **pollNonKeyPeer = off** in the *cwbinit* file, and ensure that the actively managed routers are on the list of key devices.

Clean Up Log Files

If CiscoWorks Blue has been running for a long time, some of the log files might grow quite large and impact performance. You can clean up the log files by running the **cwb maintenance** command manually or schedule maintenance as a cron job by customizing the /opt/CSCOcb/etc/cwbinit file and running the **cwb start maintenance** command. See "Database and Log File Maintenance" section on page D-2 for more details about this command.

Note that the **cwb maintenance** command stops and restarts all of the CiscoWorks Blue processes. If you would prefer to keep the CiscoWorks Blue processes active, you may clean up some of the log files manually. The safest way is to save a copy of the files, then remove the file contents, as shown in the following set of commands:

```
cp /opt/CSCOcwbC/apache/logs/access_log
/opt/CSCOcwbC/apache/logs/access_log.bak
cat /dev/null > /opt/CSCOcwbC/apache/logs/access_log

cp /opt/CSCOcwbC/apache/logs/error_log
/opt/CSCOcwbC/apache/logs/error_log.bak
cat /dev/null > /opt/CSCOcwbC/apache/logs/error_log

cp /opt/CSCOcb/logs/cwbcmd.log /opt/CSCOcb/logs/cwbcmd.log.bak
cat /dev/null > /opt/CSCOcb/logs/cwbcmd.log

cp /opt/CSCOcb/logs/DataBase.log /opt/CSCOcb/logs/DataBase.log.bak
cat /dev/null > /opt/CSCOcb/logs/DataBase.log
```

CHAPTER 10

Event Notification Messages

This chapter provides information on the Maps event notification messages. The APPN/SNASw and DLSw Maps applications send event notification messages to the workstation network management system (NMS) when changes in network status occur. These outage may be detected by SNMP traps sent by IOS routers, or by CiscoWorks Blue polling those routers for status. Event notification messages are sent as traps to the NMS through the CISCOWORKS-MIB as a cwAppLogTrap. This MIB is included with CiscoWorks Blue at /opt/CSCOcb/etc/mibs/CISCOWORKS-MIB.my . Event notification is controlled by the event values kept in the *cwbinit* file.

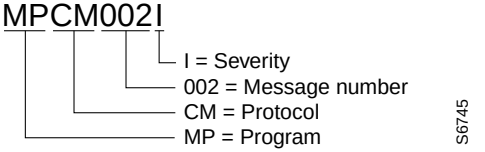
For more information, see the "Using the cwbinit Preferences File" section on page 8-6 section in Chapter 8, "Starting the User Applications."

This chapter contains the following main sections:

Event Notification Message ID Syntax

Each notification message has an eight-character message ID followed by a text string. The message ID has the syntax shown in Figure 10-1.

Figure 10-1 Syntax of Event Notification Message



Where:

Severity indicates the severity of the problem that caused the message to be issued.

- **I** is an information message.
- **W** is a warning message.

Message number is a three-digit message identification number.

Protocol is a two-character protocol ID that indicates to which protocol the event notification message applies:

- **CM** applies to both APPN/SNASw and DLSw.
- **AP** applies to APPN/SNASw.
- **DL** applies to DLSw.

Program is a two-character program ID that indicates which program issued the message:

- **MP** indicates that Maps issued the message.
- **SV** indicates that the Maps SNA Host component issued the message.
- **TR** indicates that the CiscoWorks Blue trap daemon issued this message, after receiving a trap from a router.

Event Notification Message List

This section lists the messages in numerical order by their message IDs. The messages are listed in the following sections:

APPN/SNASw Messages

The following error messages are issued by APPN/SNASw:

`MPAP001I APPN/SNASw DLUR Node dlur_node established CPSVRMGR session with DLUS Node dlus_node`

Where:

dlur_node is the DLUR node.

dlus_node is the DLUS node.

Explanation
An APPN/SNASw DLUR node (*dlur_node*) has established a CPSVRMGR session with the DLUS node (*dlus_node*), and the **eventgen_dlur** event value in the *cwbinit* file is set to ON.

`MPAP002W APPN/SNASw DLUR Node dlur_node lost CPSVRMGR session with DLUS Node dlus_node`

Where:

dlur_node is the DLUR node.

dlus_node is the DLUS node.

Explanation
An APPN/SNASw DLUR node (*dlur_node*) has lost a CPSVRMGR session with the DLUS node (*dlus_node*), and the **eventgen_dlur** event value in the *cwbinit* file is set to ON.

`MPAP003W APPN/SNASw DLUR Node dlur_node definition to DLUS Node dlus_node deleted.`

Where:

dlur_node is the DLUR node.

dlus_node is the DLUS node.

Explanation
The definition of an APPN/SNASw DLUR node (*dlur_node*) has been deleted to the DLUS node (*dlus_node*), and the **eventgen_dlur** event value in the *cwbinit* file is set to ON.

MPAP004I APPN/SNASw APPN/SNASw network CP-CP TG *tg_number* from *cp_name_1* to *cp_name_2* operational

Where:

tg_number is the TG number.

cp_name_1 is the CP name of the first node.

cp_name_2 is the CP name of the second node.

Explanation
An APPN/SNASw network CP-CP transmission group (*tg_number*) from the node identified as *cp_name_1* to the node identified as *cp_name_2* has become operational, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

MPAP005W APPN/SNASw network CP-CP TG *tg_number* from *cp_name_1* to *cp_name_2* inactive

Where:

tg_number is the TG number.

cp_name_1 is the CP name of the first node.

cp_name_2 is the CP name of the second node.

Explanation
An APPN/SNASw network CP-CP transmission group (*tg_number*) from the node identified as *cp_name_1* to the node identified as *cp_name_2* has become inactive, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

`MPAP006I APPN/SNASw endpoint CP-CP TG` *tg_number* `from` *cp_name_1* `to` *cp_name_1* `operational`

Where:

tg_number is the TG number.

cp_name_1 is the CP name of the first node.

cp_name_2 is the CP name of the second node.

Explanation
An APPN/SNASw endpoint CP-CP transmission group (*tg_number*) from the node identified as *cp_name_1* to the node identified as *cp_name_2* has become operational, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

`MPAP007W APPN/SNASw endpoint CP-CP TG` *tg_number* `from` *cp_name_1* `to` *cp_name_2* `inactive`

Where:

tg_number is the TG number.

cp_name_1 is the CP name of the first node.

cp_name_2 is the CP name of the second node.

Explanation
An APPN/SNASw endpoint CP-CP transmission group (*tg_number*) from the node identified as *cp_name_1* to the node identified as *cp_name_2* has become inactive, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

`MPAP008I APPN/SNASw Node` *node_name* `link` *link_name* `active`

Where:

node_name is the APPN/SNASw node.

link_name is the link name.

Explanation
On an APPN/SNASw node (*node_name*), a link (*link_name*) has become active, and the **eventgen_link** event value in the *cwbinit* file is set to ON.

`MPAP009W APPN/SNASw Node` *node_name* `link` *link_name* `inactive`

Where:

node_name is the APPN/SNASw node.

link_name is the link name.

Explanation On an APPN/SNASw node (*node_name*), a link (*link_name*) has become inactive, and the **eventgen_link** event value in the *cwbinit* file is set to ON.

`MPAP010W APPN/SNASw Node` *node_name* `link` *link_name* `deleted`

Where:

node_name is the APPN/SNASw node.

link_name is the link name.

Explanation On an APPN/SNASw node (*node_name*), a link (*link_name*) has been deleted, and the **eventgen_link** event value in the *cwbinit* file is set to ON.

`MPAP011I APPN/SNASw Node` *node_name* `port` *port_name* `active`

Where:

node_name is the APPN/SNASw node.

port_name is the port name.

Explanation On an APPN/SNASw node (*node_name*), a port (*port_name*) has become active, and the **eventgen_port** event value in the *cwbinit* file is set to ON.

`MPAP012W APPN/SNASw Node` *`node_name`* `port` *`port_name`* `inactive`

Where:

node_name is the APPN/SNASw node.

port_name is the port name.

Explanation On an APPN/SNASw node (*node_name*), a port (*port_name*) has become inactive, and the **eventgen_port** event value in the *cwbinit* file is set to ON.

`MPAP013W APPN/SNASw Node` *`node_name`* `port` *`port_id`* `deleted`

Where:

node_name is the APPN/SNASw node.

port_id is the port ID.

Explanation On an APPN/SNASw node (*node_name*), a port (*port_id*) has been deleted, and the **eventgen_port** event value in the *cwbinit* file is set to ON.

`MPAP014I APPN/SNASw network data TG` *`tg_number`* `from` *`node_name_1`* `to` *`node_name_2`* `operational.`

Where:

tg_number is the TG number.

node_name_1 is the name of the first node.

node_name_2 is the name of the second node.

Explanation An APPN/SNASw network transmission group without CP-CP sessions (*tg_number*), from *node_name_1* to *node_name_2* has become operational, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

`MPAP015W APPN/SNASw network data TG` *tg_number* `from` *node_name_1* `to` *node_name_2* `inactive.`

Where:

tg_number is the TG number.

node_name_1 is the name of the first node.

node_name_2 is the name of the second node.

Explanation An APPN/SNASw network transmission group without CP-CP sessions (*tg_number*), from *node_name_1* to *node_name_2* has become inactive, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

`MPAP016I APPN/SNASw endpoint data TG` *tg_number* `from` *node_name_1* `to` *node_name_2* `operational`

Where:

tg_number is the TG number.

node_name_1 is the name of the first node.

node_name_2 is the name of the second node.

Explanation An APPN/SNASw endpoint transmission group without CP-CP sessions (*tg_number*), from *node_name1* to *node_name2* has become operational, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

`MPAP017W APPN/SNASw endpoint data TG` *tg_number* `from` *node_name_1* `to` *node_name_2* `inactive`

Where:

tg_number is the TG number.

node_name_1 is the name of the first node.

node_name_2 is the name of the second node.

Explanation An APPN/SNASw endpoint transmission group without CP-CP sessions (*tg_number*), from *node_name1* to *node_name2* has become inactive, and the **eventgen_tg** event value in the *cwbinit* file is set to ON.

Messages Common to APPN/SNASw or DLSw

The following messages are issued by either APPN/SNASw or DLSw:

`MPCM001W Router router not responding to SNMP poll request`

Where:

router is a router name or IP address.

Explanation An APPN/SNASw or DLSw router has stopped responding to an SNMP network management poll, and the **eventgen_device** event value in the *cwbinit* file is set to ON.

`MPCM002I Router router responding to SNMP poll request`

Where:

router is a router name or IP address.

Explanation
An APPN/SNASw or DLSw router has started responding to an SNMP network management poll, and the **eventgen_device** event value in the *cwbinit* file is set to ON.

Event Traps Received from Cisco IOS

CiscoWorks Blue converts APPN/SNASw and DLSW traps received in Cisco IOS and translates them to a more readable format so that the affected resource can be identified. To take advantage of this feature, SNASw and DLSw routers must be configured to send Cisco IOS traps to the CiscoWorks Blue workstation. See the "Configuring Trap Destinations in Cisco IOS Routers" section on page 2-10 for information on configuring the trap destination and enabling DLSw traps.

The following shows the Cisco IOS traps and the resulting message included in the traps generated by CiscoWorks Blue.

appnLocalTgOperStateChangeTrap

```
TRAP001I APPN/SNASw Local TG <TG number> to <Destination node> state
is Operational
TRAP002W APPN/SNASw Local TG <TG number> to <Destination node> state
isNonOperational
```

appnLocalTgCpCpChangeTrap

```
TRAP003I APPN/SNASw Local TG <TG number> to <Destination node> CP-CP
sessions state is Active
TRAP004W APPN/SNASw Local TG <TG number> to <Destination node> CP-CP
sessions state is Not Active.
```

appnOperStateChangeTrap

```
TRAP005I APPN/SNASw Port <port name> state is Active.
TRAP006W APPN/SNASw Port <port name> state is Inactive.
```

appnLsOperStateChangeTrap

```
TRAP007I APPN/SNASw Link <link name> state is Active.
TRAP008W APPN/SNASw Link <link name> state is Inactive.
```

dlurDlusStateChangeTrap

```
TRAP009I DLUR/DLUS session to <DLUS name> state is Active.
TRAP010W DLUR/DLUS session to <DLUS name> state is Reset.
```

cdeTrapTConnUpDown

```
TRDL011I DLSw Connection State to DLSw peer <DLSw peer IP address is
Connected.
TRDL012W DLSw Connection State to DLSw peer <DLSw peer IP address is
Disconnected.
```

cdeTrapCircuitUpDown

```
TRDL013I DLSw Circuit State between local <mac address> and Remote mac
address is Connected.
TRDL014W DLSw Circuit State between local <mac address> and Remote mac
address is Disconnected.
TRDL015I DLSw Circuit State for PU <PU name> is Connected.
TRDL016W DLSw Circuit State for PU <PU name> is Disconnected.
```

DLSw Messages

The following messages are issued by *cwbdlswpollerd*:

`MPDL001I Router router1 established new DLSw peer connection with router router2`

Where:

router1 is the host name or IP address of the first router.

router2 is the host name or IP address of the second router. This value can also be a question mark (?) if the second router's IP address is 0.

Explanation A DLSw router (*router1*) has established a new peer connection with another DLSw router (*router2*), and the **eventgen_dlswpeercxn** event value in the *cwbinit* file is set to ON.

`MPDL002W Router router1 lost DLSw peer connection with router router2`

Where:

router1 is the host name or IP address of the first router.

router2 is the host name or IP address of the second router. This value can also be a question mark (?) if the second router's IP address is 0.

Explanation A DLSw router (*router1*) has lost a peer connection with another DLSw router (*router2*), and the **eventgen_dlswpeercxn** event value in the *cwbinit* file is set to ON.

`MPDL003I Router router1 recovered DLSw connection with router router2`

Where:

router1 is the host name or IP address of the first router.

router2 is the host name or IP address of the second router. This value can also be a question mark (?) if the second router's IP address is 0.

Explanation A DLSw router (*router1*) recovered a broken peer connection with another DLSw router (*router2*), and the **eventgen_dlswpeercxn** event value in the *cwbinit* file is set to ON.

`MPDL004I Router router1 established new DLSw circuit local_mac local_sap remote_mac remote_sap with router router2`

Where:

router1 is the host name or IP address of the first router.

local_mac is the MAC of the local router.

local_sap is the SAP of the local router.

remote_mac is the MAC of the remote router.

remote_sap is the SAP of the remote router.

router2 is the host name or IP address of the second router. This value can also be a question mark (?) if the second router's IP address is 0.

Explanation
A DLSw router (*router1*) has established a new DLSw circuit with another DLSw router (*router2*). The circuit is specified by the *local_mac, local_sap, remote_mac, and remote_sap*. The **eventgen_dlswcircuit** event value in the *cwbinit* file is set to ON.

`MPDL005W Router router1 lost DLSw circuit local_mac local_sap remote_mac remote_sap with router router2`

Where:

router1 is the host name or IP address of the first router.

local_mac is the MAC of the local router.

local_sap is the SAP of the local router.

remote_mac is the MAC of the remote router.

remote_sap is the SAP of the remote router.

router2 is the host name or IP address of the second router. This value can also be a question mark (?) if the second router's IP address is 0.

Explanation

A DLSw router (*router1*) has lost a DLSw circuit with another DLSw router (*router2*). The circuit is specified by the *local_mac*, *local_sap*, *remote_mac*, and *remote_sap*. The **eventgen_dlswcircuit** event value in the *cwbinit* file is set to ON.

`MPDL006I Router` *router1* `recovered DLSw circuit` *local_mac local_sap remote_mac remote_sap* `with router` *router2*

Where:

router1 is the host name or IP address of the first router.

local_mac is the MAC of the local router.

local_sap is the SAP of the local router.

remote_mac is the MAC of the remote router.

remote_sap is the SAP of the remote router.

router2 is the host name or IP address of the second router. This value can also be a question mark (?) if the second router's IP address is 0.

Explanation

A DLSw router (*router1*) has recovered a DLSw circuit with another DLSw router (*router2*). The circuit is specified by the *local_mac, local_sap, remote_mac,* and *remote_sap*. The **eventgen_dlswcircuit** event value in the *cwbinit* file is set to O N.

SNA Host Messages

The following messages are issued by the SNA host component:

`SVST001W SNA Host detected a PU name change for` *`pu_name`* `with IDBLK/IDNUM` *`value`*

Where:

`pu_name` is the name of a PU.

`value` is the hexadecimal IDBLK/IDNUM value.

Explanation

The Maps SNA Host component found a PU (*`pu_name`*) whose hexadecimal IDBLK/IDNUM *`value`* is already in the database for another PU name. This could happen if you change the VTAM definitions of the PUs, or if there is a problem with the VTAM definition for one of these PUs.

CHAPTER 11

Troubleshooting CiscoWorks Blue Applications

This chapter provides information on detecting and correcting problems with a CiscoWorks Blue application on UNIX workstations.

This chapter includes the following main sections:

Calling Cisco TAC

When you have isolated an error to one of the CiscoWorks Blue applications, typically you notify the Cisco TAC of the problem. Before you call the Cisco TAC, use the **cwb tac** command to collect the appropriate diagnostic data and zip it for transmission to Cisco.

UNIX Workstations

To collect and zip the diagnostic data, enter the following commands:

cd /opt/CSCOcb/bin

./cwb tac

The **cwb tac** command copies information from key files and from the CiscoWorks Blue database, and packages it in the following file: */usr/tmp/cwbtac_hostname_index.tar.Z*

Where:

hostname is the actual hostname. If you set the environment variable CWB_TAC_CLIENT_ID to some value, then the hostname should be the value of this variable.

index is the next available counting number, starting with 1, for the first execution of cwb tac. The index value for the second execution of cwb tac is 2, and so on. This number is generated by looking at the existing file names; therefore, if you delete a file or change the hostname value, the counting restarts at 1. For example:

/usr/tmp/cwbtac_tblm_1.tar.Z

Submit this file, along with any other pertinent information, when you open a case with the Cisco TAC.

Specifying a Directory with the cwb tac Command

The **cwb tac** command lets you specify a directory for saving the command output.

The **cwb tac** command runs the CiscoWorks Blue TAC collection program to collect and zip all the information you will need when you call the Cisco TAC. You must be the root user to use the **cwb tac** command.

Command	**cwb tac [-o** *outputdirectory***]**
Syntax Description	
-o *outputdirectory*	Specifies a directory in which the command output is saved. If you omit this operand, the output is saved as file *cwbtac_n.tar.Z* in a temporary directory, where the *n* is increased for each successive use. The **cwb tac** command searches for a temporary directory in this order: */usr/tmp*, */var/tmp*, */tmp*. You can specify an output directory in which to save the output of the **cwb tac** command: • You can specify an absolute directory by preceding the path with a / character. If the specified directory does not exist, the **cwb tac** command prompts you to create it. The following command saves the zipped file as */usr/cwblue/cwbtac_1.tar.Z*: **cwb tac -o /usr/cwblue** • You can specify a relative directory. This directory is always relative to */opt/CSCOcb/etc*. The following command saves the zipped file as */opt/CSCOcb/etc/tac/cwbtac_1.tar.Z*: **cwb tac -o tac**

General Troubleshooting

If the application fails to operate correctly, perform the generalized diagnostic tasks as the root user. The diagnostic tasks are described in the following section.

An Exception Occurs when Collecting Data for TAC

If you are collecting data for TAC and osfind displays the following exception error message, you can ignore the message:

```
CORBA Exception during execution of osfind: EXCEPTION
ObjLocation::Fail
{
reason:
4
}
```

Customer ISTEXCCS Exit Driven With Unrequested Vector Types

VTAM provides customers with the ability to define additional information about dynamic PUs by using the ISTEXCCS configuration exit. This exit can select which type of information it will receive from VTAM and can elect to receive information on dynamic or static resources. The exit manager provided with the CiscoWorks Blue products may incorrectly drive customer exits with information the exit did not request from VTAM.

For example: A customer exit registers to receive only information on dynamic resources may receive information on static resources once the CiscoWorks Blue products have been installed on the system.

Work around

Customer can modify their exit to ignore unrequested types of resources.

Directory Name is Invalid but the Installer Still Creates It

During installation, you are prompted to select an installation directory. If you do not accept the default directory and choose to create a new directory, use valid naming conventions, such as 8-character names without any spaces. An error can occur in which the installer indicates the directory name is invalid but it still creates the directory.

DLC Information is Missing for Certain Physical Units

Informational messages, NSP040 and NSP041, can appear indicating that physical units (PU) are missing or are displayed incorrectly. These messages are provided by the NSPOPEN application and appear in the mainframe system log. SNA View determines the underlying resources used to connect these PUs to the mainframe.

```
NSP040 Resource RESOURCE not found in database:VSAM RC=RC errno=ERRNO
NSP041 Unable to obtain DLS information for RESOURCE
```

For more information on these messages, see Chapter 6 in *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide*.

Dynamic Logical Units are Missing

In certain cases, CiscoWorks Blue SNA View is unable to collect status changes dynamically on certain types of logical units (LU). Status information on dynamically-defined LUs is collected only when a host discovery is requested or a VTAM message has indicated a state change has occurred on the PU.

Work around

To maintain information on dynamic LUs, you can recycle the host connection by using the **stop cwbhcid** and **start cwbhcid** commands. Or you can set up the host connection to periodically activate (v net,act,id=puname) PUs that support dynamic LUs.

Dynamic Physical Unit Construction Rejected After Installing CiscoWorks Blue ISTEXCCS

Customers can create PUs dynamically without using the ISTEXCCS exit to define additional information on these types of PUs. In this case, the CiscoWorks Blue exit may incorrectly act as the primary exit and reject the creation of the PU.

Work around

None. Contact TAC to install the latest version of CiscoWorks Blue exits that support this configuration.

Logical Unit Status is Incorrect

The status of an LU is incorrect in a Session Connectivity page. The CiscoWorks Blue SNA Resource Information page produces session lists that contain the status of LUs *at the time the request was issued*. If the status of the affected LU changes while either the Session List or Session Connectivity page are displayed, the changed status of the LU is not updated and displayed.

Work around

You can click the **Reload** button from the Session List or the Session Connectivity page to update the LU status or you can re-issue the entire request from the SNA Resource Information page.

Messages NSP040 and NSP041 Issued to the System Log

In some cases, CiscoWorks Blue SNA View may provide incorrect information on switch PUs. This problem appears as PUs displayed with incorrect or incomplete session path information. In addition, the NSPOPEN mainframe application will generate messages NSP040 and NSP04 to the system log for these resources. These messages are generated when the CiscoWorks Blue ISTEXCCS exit fails to collect the necessary information on the switched resources.

This exit failure can occur when a customer exit is present and is being used to define additional information on dynamic PUs. If the customer exit provides a vector to define in which major node to create the new PU, the CiscoWorks Blue exit may reject the processing for this PU.

Work Around

None. Contact TAC to install the latest version of CiscoWorks Blue exits that support this configuration.

Router Discovery Fails in SNA View because HPOV (Version 6) Changes the SNMP Port to 8161

An early release of HPOV, version 6, might set the SNMP port to 8161 in the *services* file. This port number change causes other SNMP-based applications, such as CiscoWorks Blue Maps and SNA View to fail.

You can use the following workarounds:

Step 1 Edit the */etc/services* file.

Step 2 Change the SNMP port from 8161 to 161. Or apply the latest HPOV consolidated patch.

TCP Failure on the Mainframe Requires you to Restart NSPOPEN

In some cases, TCP/IP failure on the mainframe requires that you restart the NSPOPEN application. This problem can occur only for those using TCP/IP. If you are using LU 6.2, you can ignore this problem.

Work around

You can automate NetView to detect a failure in TCP/IP and issue the command to stop NSPOPEN. You can automate NetView to detect when TCP/IP is restarted and issue the command to start NSPOPEN.

Unable to Launch the Administration Application to Collect Information for TAC

If you want to use the Tools menu in the Administration application to collect diagnostic data for TAC, but are unable to launch the Administration application, use the following workaround:

Step 1 Open a command-line prompt.

Step 2 Change the directory to the installation directory by entering the following:

cd <name of install directory> \CSCOcb\bin

Step 3 Enter the following command:

cwb tac

Unable to Start Database Processes on UNIX Workstations

If you installed CiscoWorks 2000 and then CiscoWorks Blue in the same shell on UNIX systems, you can receive an error in which CiscoWorks Blue points to the CiscoWorks 2000 database. If this error occurs, the SQLAnywhere DB processes will not start and you will receive the following message:

```
px.log is not a database.
```

To recover, exit the shell in which you installed the applications and run the **cwb stop all** command followed by the **cwb start servers** command. This action will point CiscoWorks Blue to the appropriate database and start the servers.

Unable to Start Process Manager on UNIX Workstations

If you are unable to start the Process Manager, if you get “out of space” errors trying to start other CiscoWorks Blue processes, or if you get java exceptions with the message “out of memory,” you might need more physical memory, or to swap space in the workstation. Alternatively, especially on HP-UX because of low defaults, try increasing the kernel parameters beyond the minimal values required by Maps and SNA View.

Using the Process Manager Client on UNIX Workstations

Use the Process Manager client (**cwb start ProcMgrClient**) or launch from the Administration application to verify that all required processes are running.

Using the cwb show status Command on UNIX Workstations

Use the **cwb show status** command as a UNIX command line alternative to using the PM client. On UNIX workstations, use the **cwb show status** command in the */opt/CSCOcb/bin* directory to verify that all the servers and processes are active:

cd /opt/CSCOcb/bin

./cwb show status

You can then use the **cwb start** command to start any servers or processes that are not running, and you can start the Process Manager client to monitor them, as described in Chapter 4, "Monitoring and Controlling CiscoWorks Blue Applications."

Using the Message Log Viewer

Use the Message Log Client (**cwb start MsgLogClient**) or launch the Message Log Client from the Administration application to view messages as they are logged by CiscoWorks Blue processes.

UNIX Workstations

If you have not already started the Message Log client, you will have to view these messages in the message log files in */opt/CSCOcb/logs* on UNIX workstations.

Using the cwb verify Command

UNIX Workstations

Use the **cwb verify** command in the */opt/CSCOcb/bin* directory on UNIX workstations or launch the verification tool from the Administration application to verify that all the installation tasks were completed successfully.

Web Server Startup Errors on Solaris

While starting the web server, an error may occur in which *CWBHTTPAdapter* or *CWBDBAdapter* does not start. However, after automatic retries, the *CWBHTTPAdapter* or *CWBDBAdapter* process starts.

If the adapters start after some automatic retries, this errors indicate a temporary condition that has been automatically corrected.

Processes Do Not Start

The Process Manager is running, but when you issue the **cwb show status** command, the output shows all CWBlue processes in the *Initial* state whereas the CWBMsgLogServer is in the *Starting* state. The MsgLogServer gets the following message during startup:

```
Unable to bind to Process Manager Server
```

This message is followed by a detailed CORBA System Exception information.

Work around

The problem appears to be a third-party package error. A workaround might be available by changing the **localhost** entry in the */etc/hosts* file. Check the */etc/hosts* file. The **localhost** entry should be the first uncommented entry in the */etc/hosts* file as shown in the following examples:

```
# comment line in hosts file
127.0.0.1       localhost loghost
```

or

```
127.0.0.1       localhost
```

To make the **localhost** entry the first entry, change the */etc/hosts* file as shown below:

Step 1 Become the root user:

su root

Step 2 Edit the */etc/hosts* file.

Step 3 Either add this line as the first entry or move this line to the first entry.

```
127.0.0.1       localhost [loghost]
```

Note If this entry exists in the file, there might be additional aliases on this line, before or after the **localhost** entry, such as the **loghost** alias. Keep the line intact when you move it to the first entry position.

Step 4 Stop all servers:

/opt/CSCOcb/bin/cwb stop all

Step 5 Start all servers:

/opt/CSCOcb/bin/cwb start servers

Troubleshooting the DLSw and RSRB Applications on UNIX workstations

This section describes some general DLSw and RSRB troubleshooting procedures for initial problem resolution for those using UNIX workstations, and then lists specific symptoms and possible remedies.

SNMP Request Errors

If there is an SNMP error while requesting information from the router, log on to the router and check for the following command in the current configuration:

snmp-server community *read_community_string* **RO**

The *read_community_string* should match the read community string used by Maps. You can check and edit this value by clicking a router icon with the right mouse button, and then selecting **Edit > Modify**.

The default SNMP server packet size is 1500. If the packet size is too low, then some commands might fail. If commands fail, you can raise the packet size to 8192.

You can use the Maps application menu bar to rediscover, add, or delete the router, as shown below.

- Select **Edit > Rediscover** from the menu bar to rediscover the router.
- Select **Edit > Delete** from the menu bar to delete the router.
- Select **Edit > Add** from the menu bar to add the router.

SNMP Traps

If a trap occurs, but the status change is not reflected in the map, check the router configuration, as described in the "Configuring Trap Destinations in Cisco IOS Routers" section on page 2-10 and use the Process Manager to see the status of the *cwbtrapd* process.

Diagnosing DLSw and RSRB Symptoms

For those using UNIX workstations, Figure 11-1 lists symptoms that your DLSw or RSRB application might demonstrates and refers you to various chapter sections for diagnostic techniques to resolve the problems.

Figure 11-1 DLSw and RSRB Troubleshooting Symptoms

For this symptom...	See this section...
Device does not appear on the map	Device Not on Map, page 11-14.
Global view is empty	Blank Map, page 11-13.
Incorrect device information	Device Information Obsolete, page 11-15.
Nodes not synchronized	Nodes Not Synchronized, page 11-16.
Unexpected dialog box prompt appears	DLSw and RSRB Error Messages on UNIX Workstations, page 11-17.

Blank Map

If the RSRB or DLSw map is blank, synchronization with the network management system or seed file might have failed. Ensure that network devices were discovered by the network management system.

If a DLSw key routers view is blank, select **Edit > Key Devices** from the menu bar to ensure that you have designated routers as key devices in the seed file. If the key routers view is still blank, select **View > Global** to display a global view.

SunNet Manager maintains a separate device database for each user. In this case, you must use the RSRB or DLSw application from the username whose database you want to synchronize.

Also, you can try logging in to the Sybase server to check whether the devices in the seed file are also in the database. The following procedure describes how to check the database with the **isql** command.

Step 1 Issue the **source** command to set the database environment variables:

source /opt/CSCOcwbC/db/CSCOcwb/dbenv

If the source command produces errors, you must manually set the database environment variables as they are set in the */opt/CSCOcwbC/db/CSCOcwb/dbenv* script.

Step 2 Then issue the **isql** command:

$SYBASE/bin/isql -Usnasuper -Psnarsrb

1> select * from snasuper.devices

2> go

You should see all devices that are in your seed file.

Device Not on Map

If a device fails to appear on the map, the discovery daemon might have failed. Perform the following steps:

Step 1 Use the **isql** command, as shown below, to verify the device's entry in the Sybase Devices table. This example is for a database named SNA.

```
$SYBASE/bin/isql -Usnasuper -Psnarsrb
```

1> select * from snasuper.devices where device_name=*device_name*

2> go

1> quit

Step 2 If the device named *device_name* is not in the Devices table, check for its existence in the network management system database or the seed file. If the device is in the Devices table, verify that it is running the correct release of Cisco IOS software and that you can ping the device from the network management system. Select **Edit > Modify** and enter the device name and correct read community string.

Step 3 Use **Edit > Add Device** to add the device to the map. The RSRB or DLSw application attempts to discover a newly added device automatically.

Step 4 Use the **ping** command to verify that you can locate the device.

Step 5 Check whether SNMP is configured on the router and verify the read community string. SNMP must be configured on the router for DLSw and RSRB.

Step 6 Check the access list in the router configuration to verify that the IP address can be reached.

Device Information Obsolete

If a device appears on the map but the information about it appears to be out of date, use the following procedure to delete the obsolete information:

Step 1 Select **Edit > Rediscover Device(s)** to rediscover the device.

Step 2 Use the Process Manager to reset the poller and monitor daemons.

If the problem remains unresolved, ensure that the poller is active. If a network management system is present, ensure that both the network management system trap daemon and the *cwbtrapd* process are active. For more information, see the "DLSw and RSRB Error Messages on UNIX Workstations" section on page 11-17.

Nodes Not Synchronized

If the nodes in your network are not synchronized with your database, try one of the following procedures.

Procedure 1

Step 1 Select all the devices on the map and rediscover them:

Step 2 Select **Layout > See All**.

Step 3 Select all the devices on the map.

Step 4 Select **Edit > Rediscover Device(s)**.

Procedure 2

Use the following commands to remove all entries from the database tables:

cd /opt/CSCOCB/bin

./cwb clear db

For information about the **cwb clear db** command, see Appendix D, "CiscoWorks Blue Commands and Processes." Rerun the discovery processes to repopulate the database tables. In Maps, select **Administration > Discover** from the menu bar.

DLSw and RSRB Error Messages on UNIX Workstations

For those using UNIX workstations, the following error messages are issued to the message box in the RSRB and DLSw Motif applications and to the message log:

```
Cannot log into the database.
```

Explanation
RSRB or DLSw either cannot get to the data server or cannot log in.

Action
Check the environment variables in */opt/CSCOcb/etc/runprocess*; try to log in to the database server from a separate window and check the transaction log. Then try to restart the application.

```
Current view_name view type conflicts with reserved name prefix
of file.
Save map file filename Failed!
```

Where:

view_name is the name of the view that you are trying to save to a file:

- For APPN/SNASw the *view_name* can be Global, Local, or Port.
- For DLSW the *view_name* can be Global, Key Devices, Focus Peer, PU Dependency, or LU Dependency.
- For RSRB the *view_name* can be Global, Virtual Ring, Focus Peer, PU Dependency, or LU Dependency.

filename is the name of the file in which you are trying to save the view.

Explanation You tried to use **File > Save As** to save a map to a file, but the file prefix is one of the reserved Maps file prefixes. Maps reserves the following file prefixes:

- For APPN/SNASw: Local_, Port_
- For DLSW: Key_Devices_, Focus_

- For RSRB: VR_, Focus_
- For all: Global_, PU_, LU_

Action Do not use **File > Save As** to save to a file with one of the reserved prefixes.

`Database initialization failure.`

Explanation
RSRB or DLSw failed to connect to the network management system database before starting the discovery daemon.

Action
Verify the integrity of the network management processes. If you have HP OpenView or NetView installed, you can use the **ovstatus** command, which typically is located in the */usr/OV/bin* or */opt/OV/bin* directory. The **ovstatus** command displays the status of daemons and processes. You can ensure that all network management daemons are running, and restart those that are not.

`device_name` `already exists.`

Explanation
When you tried to add a device to the database, the device you specified already had an entry in the database.

Action
You can delete the device and add it again using the **Edit** item on the Motif menu bar or using the Administration application.

device_name no such device.
device_name failed to add.

Explanation
The *device_name* is not known to the operating system or to the domain name server.

Action
Try to ping the device. If that fails, check for the correct case. Check to see whether the domain name server has been configured. Verify that the device name is in the */etc/hosts* file.

Discovery failed.

Explanation
RSRB or DLSw failed to query network devices.

Action
If you have HP OpenView or NetView installed, you can use the **ovstatus** command, which typically is located in the */usr/OV/bin* or */opt/OV/bin* directory. The **ovstatus** command displays the status of daemons and processes. You can ensure that all network management daemons are running, and restart those that are not running.

Invalid view type

Explanation When switching views, for example from global view to focus view, a correct filename and format is read, but the view type in the file is wrong. For example, the map is changing to a focus view, but the view type says it is a virtual ring view.

Action Delete or move the particular map file.

`No community string`

Explanation
RSRB or DLSw does not know the community string for this router.

Action
Use the **Edit > Modify** menu item or the Administration application to set the correct community string.

`No response from update server.`

Explanation
The monitor daemon is not running.

Action
Use the Process Manager or the **cwb start** command to start the monitor daemon.

`Port already in use.`

Explanation
A copy of the monitor daemon is already running on the workstation, or some other program is using this port.

Action
If another copy of the monitor daemon is already running, this is an informational message. No action is necessary. If another program is using this port, you can edit the **runprocess** script and change the setting of the **-u** monitor port option for the **case dlsw** or **case rsrb** sections.

`Reading map file` *`filename`*`. Incorrect format or version. Open file Failed!`

Explanation You are reading a map file with an incorrect format or version. This happens when a map file format changes between versions of Maps and an attempt is made to try to read the incompatible format.

Action Delete or move the particular map file.

```
Rediscover Device(s) failed.
```

Explanation
The SNMP query to a device was not successful. Either the device is no longer reachable from the network management workstation or it is not responding to the SNMP query.

Step 1 Use the **ping** command to see whether the router is active.

Step 2 Use the **telnet** command to log in to the router to check the router configuration. Ensure that the router is configured for the protocol you are using and configured for SNMP, and that the read community string is correct.

Troubleshooting the SNA Host Component

This section contains the following information:

- The "Overview of Workstation Error Handling" section on page 11-22 provides basic information about SNA LU and PU error processing and a method for generating supplemental debugging data.
- The "Workstation-to-Mainframe Connectivity Problems" section on page 11-22 describes problems with the a connection between the workstation and the mainframe.

- The "Problems Related to Discovery and Status Management" section on page 11-24 discusses problems related to discovery and status management.
- The "Configuration File Problems" section on page 11-26 describes problems that are not related to any single component; such problems can involve environment variables, configuration files, and file security.

Overview of Workstation Error Handling

The LU and PU processes relay operating and error messages to the Message Log Server in which the management platform was started. You can view these messages, as they are logged, using the Message Log client.

All SNA host LU and PU errors are in the following form:

CWC*xxxnnn message_text*

Where:

xxx is a 2- or 3-letter message category.

nnn is a 3-digit numeric identifier.

For example:

```
CWC0006W Socket connect failed, will retry momentarily.
```

This chapter provides a detailed description of each message and, if appropriate, a recommended user response.

Workstation-to-Mainframe Connectivity Problems

This section describes problems related to communications between the mainframe and workstation components in TCP/IP and LU 6.2 environments.

TCP/IP Connectivity Problems

If the Host Connection Interface or the Host Command Server will not initialize successfully, perhaps due to communications problems between the workstation and mainframe. Perform the following procedures.

On the Workstation

Step 1 Verify that the *SVMF_AGENT_ADDR* configuration parameter (in the */opt/CSCOcb/etc/svopen_config_domain* file) is set to the correct IP address or host name of the mainframe.

Step 2 Verify the network connection from the workstation to the mainframe by issuing a TCP/IP **ping** command.

Step 3 Verify that the *SVMF_HCI_AGENT_PORT* and the *SVMF_CMDS_AGENT_PORT* configuration parameters (in the */opt/CSCOcb/etc/svopen_config_domain* file) are set correctly on the workstation. These configuration parameter values must match the parameter card values for the TCP subtask on the mainframe.

On the Mainframe

Step 1 For IBM TCP/IP connections, verify that the TCP subtask for your requested ports is active. Issue the **F NSPOPEN,SHOW TASK** command and look for the desired ports to confirm that the TCP subtask's state is READY. If the TCP subtask's state is not READY, use the **INIT** command to activate the TCP subtask.

Step 2 Verify that another workstation is not connected to the TCP subtask. Issue the **F NSPOPEN,SHOW CONN** command to confirm that there is no connection for the relevant TCP subtask. If another workstation is connected, choose a different pair of port numbers and reconfigure.

LU 6.2 Connectivity Problems

The best source of information for debugging LU 6.2 problems is the job log of the CiscoWorks Blue mainframe component. It will contain error messages written by the SERVER subtask.

For LU 6.2 connections, verify that the associated SERVER subtask is active. Issue the **F NSPOPEN,SHOW TASK** command to confirm that the SERVER subtask's states are UP. See the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide* for more details on problems and solutions with the SERVER subtask and LU 6.2 communications.

Problems with the SNA Communications Software

You can find helpful information for troubleshooting LU 6.2 connectivity problems in audit message logs, error message logs, and link traces.

Configuring Audit and Error Logging

The SNA communications software generates audit and error messages during operation and writes them to files specified during configuration. See the product documentation for more details on specifying log files and message severity levels.

Starting Tracing

When you start tracing, tracing information is written to the trace files (*.tr) in addition to the diagnostic messages written to the audit and error logs. See the product documentation for more details.

Problems Related to Discovery and Status Management

Note You must have root user authority on the workstation to complete many of the tasks described here.

Problems relating to discovery and status management are described in the following sections:

- Problems Discovering Your PUs and LUs, page 11-25
- Data-Gathering Errors, page 11-25

Problems Discovering Your PUs and LUs

Discovery is a process that gathers the information on PUs and LUs for a specific domain and stores that information in the CiscoWorks Blue database. The following problems can occur:

- Connectivity Errors—To gather information for the *cwbhmond* process, a connection to the mainframe must be established. Problems can occur with this connection. For more information, see the "Workstation-to-Mainframe Connectivity Problems" section on page 11-22.
- LUs Not Discovered—When LUs are not discovered, usually a problem exists in the configuration file. In the "Configuration File Problems" section on page 11-26, review the information provided for the *INCLUDE_LUS* configuration parameter, which must be set to YES (or yes) to enable discovery of LUs. Call your mainframe system administrator or network administrator to verify that the LU_CONTROL parameter card is configured to send LU information to the workstation.

Data-Gathering Errors

The *cwbhmond* process receives updated PU information from the mainframe when a status change occurs or when a new PU is discovered. If status updates are not being received at the workstation (that is, when the status of a PU changes but the change is not reflected when the PU information is displayed), messages might not be flowing from VTAM to the mainframe application. Ask your mainframe administrator to use the following commands:

- Use the **MODIFY NSPOPEN,SHOW TASK** command to ensure that the PPI or PPO subtask and the STATUS subtask are active.
- Use the **MODIFY NSPOPEN,SHOW FLOW** command to check the INFLOW and OUTFLOW values for the PPI or PPO subtask (whichever you are using) and for the STATUS subtask. They should be greater than 0 and should increment each time a status change occurs.

This problem is described in the "Troubleshooting the Mainframe Application" chapter of the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide*.

Configuration File Problems

Configuration file errors are common sources of application failures. Each managed SNA domain has a configuration file in the */etc* directory. Each domain configuration file name is in the format *svopen_config_ domain*. These configuration files contain parameters that affect almost every aspect of SNA host functionality. Several configuration file parameters, if not correctly set, can keep workstation processes from executing properly.

Note Workstation processes retrieve parameters only once (during initialization). Therefore, after you make modifications to a configuration file, stop and restart the processes for the changes to take effect.

The following sections describe the configuration file parameters and the problems that can arise if they are not set correctly.

SVPATH

SVPATH is the path to the home directory on UNIX (*/opt/CSCOcb/snahost*).

If this variable is not properly set to the home directory, as defined during installation, workstation processes cannot locate necessary help, log, and parameter files. Most workstation processes will not initialize without a valid SVPATH parameter value.

SVMF_AGENT_ADDR

SVMF_AGENT_ADDR is the TCP/IP host name of the IBM mainframe running the mainframe application.

If this configuration parameter is not properly set, the Host Connection Interface and the Host Command Server will fail to initialize when TCP/IP is for communications between mainframe and workstation.

For example, if the value of this configuration parameter is *mickey,* but *mickey* is not a valid machine on the network, you will get the following error messages written to the Message Logger when you attempt to start the Host Connection Interface or Host Command Server:

```
CWC0037E client_bind_udp_socket() failed calling gethostbyname(),
reason: Error 0.

CWC0043E Unable to obtain host TCP/IP address from host name: mickey
CWC0048I client_bind_udp_socket() process has exited.
```

However, if **mickey** is a valid machine name, but the TCP subtask of the mainframe component is not currently running, these error messages are written to the message log if the IPCTrace message category is enabled:

```
CWC0001E server_connect_tcp_socket() failed calling connect(), reason:
Connection refused.
```

Similar error messages will be generated if the *SVMF_HCI_AGENT_PORT* and *SVMF_CMDS_AGENT_PORT* values are not set properly. These configuration parameters must match the ports defined on the mainframe program's TCP parameter card. See the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide* for more details.

SVCMD_TIMEOUT

SVCMD_TIMEOUT is the time out period, in seconds, for mainframe commands.

If this configuration parameter is set too low, then mainframe commands issued from the workstation can time out. Try to increase this parameter value.

The default value of this configuration parameter is 30 seconds. In most cases this value is sufficient. However, when the workstation-to-mainframe connection is very slow, you might need to increase this value. If this configuration parameter is set too low, the following error messages will be issued to standard error:

```
CWC0061W Timed out waiting for command response from Command Server.
CWC0064W Command not processed. Verify that the HCI and Command
Servers are active.
```

If increasing this configuration parameter does not prevent commands from timing out, ensure that the Host Connection Interface and Host Command Server are active. If they are inactive, activate them. If they are active, check the

mainframe performance group, which might be set too low. See your mainframe system administrator or see the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide* for assistance.

SVCMDS_AGENT_PORT

The server and client processes use this port for socket communications. Ensure the port is not used twice, and that it is not used by some other process.

SVHCI_STATUS_PORT

The Host Connection Interface communicates with the VTAM and MVS Servers, and the *cwbhmond* process, over these defined ports. Ensure the port is not used twice and that it is not used by some other process.

SVMF_HCI_AGENT_PORT, SVMF_CMDS_AGENT_PORT

These configuration parameters define the port values used for TCP/IP communications between the workstation and mainframe components. The Host Connection Interface and Host Command Server use these port values to establish socket communications with the TCP subtask on the mainframe. The port values specified in the configuration file on the workstation must match those defined on the TCP subtask parameter card in the mainframe component's SYSIN parameter card file. See the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide* for more information on the TCP subtask and SYSIN parameter card file.

If these configuration parameters do not match those defined on the mainframe, the workstation application will generate the following error messages on standard error when starting the Host Connection Interface and Host Command Server:

```
CWC0001E server_connect_tcp_socket() failed calling connect(), reason:
Connection refused.

CWC0007E Socket connect failed, no retry will be attempted.
CWC0048I server_connect_tcp_socket() process has exited.
```

SNA Host Workstation Messages

This section explains the messages generated by the workstation program. Each message number ends with one of the following error codes:

- E—Error message
- I—Information message
- W—Warning message

`CWC0001E` *`process`* `failed calling` *`function`*`, reason:` *`explanation`*

Where:

`process` is the process or routine.

`function` is the system socket function.

`explanation` is the text that explains the error.

Explanation A process has called a system function and that function has failed. The reason is given in the *`explanation`* field. In most cases, a system function essential to the process is missing. Without it, the process cannot continue and will exit with an error.

Action If the explanation is not clear, check to make sure the configuration file for that particular domain is defined correctly. In some cases, the error might be caused by the system load, and the process will run properly if restarted.

`CWC0002E Unable to open` *`protocol method`* `socket.`

Where:

`protocol` is the socket protocol.

`method` is either the stream or datagram method.

Explanation A process was unable to open a socket type with the indicated communication method. The process that attempted to open the socket will terminate.

Action In some cases, the error is caused by the system load, and the process will run properly if restarted.

`CWC0003E Unable to bind socket.`

Explanation A process was unable to bind an open socket. The process that attempted to bind the socket will terminate.

Action In some cases, the error is caused by the system load, and the process will run properly if you restart it.

`CWC0004E Unable to set socket to non-blocking mode.`

Explanation A process was unable to set the mode of a socket to nonblocking. Processing continues.

Action No user action is required.

`CWC0005E Error on listen for socket connection.`

Explanation A process was unable to activate a socket for connection. The process that attempted to listen for the socket connection will terminate.

Action In some cases, the error is caused by the system load, and the process will run properly if restarted.

`CWC0006W Socket connect failed, will retry momentarily.`

Explanation A process attempted to connect to another process via socket communications and failed. In most cases, the other process has not had enough time to initialize and establish the socket properly. The process will pause briefly and then reissue the connection attempt.

Action No user action is required.

`CWC0007E Socket connect failed, no retry will be attempted.`

Explanation One process attempted to connect to another process via socket communications and failed. The process that detected the error will terminate.

Action Make sure that both processes involved in the connection are executing. Make sure the configuration file for that particular domain is correctly defined. In some cases, the error is caused by the system load, and the process will run properly if restarted.

`CWC0008E Unable to get socket option: socket.`

Where:

socket is the specific socket option.

Explanation A process attempted to obtain the socket option and failed. The process that detected the error will terminate.

Action Attempt to restart the failing process.

`CWC0009E Unable to set socket option: socket.`

Where:

socket is the specific socket option.

Explanation A process attempted to set the socket option and failed. The process that detected the error will terminate.

Action Attempt to restart the failing process.

`CWC0010E process failed reading HCI socket, reason: explanation.`

Where:

process is the server process.

explanation is text that explains the error.

Explanation A server attempted to read from the Host Command Interface and failed. The server will notify its clients and then terminate.

Action Verify that the Host Command Interface server is active. In some cases, the error is caused by the system load, and the process will run properly if restarted.

`CWC0011E Failure reading` *`process`* `client UDP socket.`

Where:

`process` is the client process name.

Explanation A server process failed while reading a client's socket. The server process will terminate.

Action In some cases, the error is caused by the system load, and the process will run properly if restarted.

`CWC0012E Failure reading` *`process`* `server UDP socket, entire message not received.`

Where:

`process` is the server process.

Explanation A client process attempted to read from a server process and received only a partial message. The detecting client process will terminate.

Action Verify that the client's server process is still active and functioning properly. In some cases, the error is caused by the system load, and the process will run properly if restarted.

`CWC0013E Failure writing to` *`process`* `client UDP socket.`

Where:

`process` is the client process.

Explanation A server process failed while writing data to a client process. A server process will continue processing if a write to a client process fails.

Action Verify that the client process is still active and, if not, restart the client process repeating the desired action.

`CWC0014E Failure writing to` *`process`* `client UDP socket, entire message not sent.`

Where:

`process` is the client process.

Explanation A server process failed to send the entire data buffer to an SNA host client process. A server process will continue processing if a write to a client process fails.

Action Verify that the client process is still active and, if not, restart the client process.

`CWC0015E Failure reading SView/Open Mainframe Message Server, reason:` *`explanation`*`.`

Where:

`explanation` is text that explains the error.

Explanation The Host Connection Interface failed while attempting to read from its socket connection with the Mainframe Message Server. The Host Connection Interface server will exit, causing the termination of the majority of all SNA host processes.

Action Review text explanation of the error and verify TCP/IP support between the workstation and the mainframe in question.

`CWC0016E Lost connection with SView/Open Mainframe Message Server.`

Explanation The Host Connection Interface lost connection with the SNA host Mainframe Message Server. This message indicates that some vital process or processes on the mainframe have terminated or become unavailable. The Host Connection Interface server will exit, causing the termination of the majority of the processes.

Action Verify the status of the mainframe application and the TCP/IP support.

`CWC0017E` *`process`* `has exited due to read failure on HCI connection.`

Where:

`process` is the server process.

Explanation A server process exited because it received an error return code when it attempted to read from the Host Connection Interface socket. The server process will terminate.

Action Verify that the Host Connection Interface for that domain is active.

`CWC0018E` *`process`* `has exited due to loss of connection with the HCI.`

Where:

`process` is the server process.

Explanation A server process exited because it lost connection with the Host Connection Interface. This message indicates that the Host Connection Interface process has terminated and is no longer available. The server process terminates.

Action Verify that the Host Connection Interface for that domain is active.

`CWC0019E HCI failed sending command response to the Command Server.`

Explanation The Host Connection Interface could not send the response, to a mainframe command, back to the Host Command Server.

Action Ensure that the Host Command Server process is active on the workstation. If it is not active, start the process. If it is active, stop and restart the process.

`CWC0020E` *`process`* `failed calling` *`name`* `with errno:` *`error_number`*

Where:

`process` is the process or routine.

`name` is the LU 6.2 system routine name.

`error_number` is the error return.

Explanation The process or routine failed calling the LU 6.2 system routine and returned an error code. The process that detected the error will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 communications are configured properly.

`CWC0021E Failure opening` *`direction`* `LU 6.2 conversation.`

Where:

`direction` is inbound or outbound.

Explanation The Host Command Interface or the Host Command Server failed to open the LU 6.2 conversation with the mainframe system. The process that detected the error will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 communications are configured properly.

`CWC0022E Failure allocating direction LU 6.2 conversation.`

Where:

direction is inbound or outbound.

Explanation The Host Command Interface or the Host Command Server failed to allocate the LU 6.2 conversation with the mainframe. The process that detected the error will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 communications are configured properly.

`CWC0023E Failure reading over direction LU 6.2 conversation.`

Where:

direction is inbound or outbound.

Explanation The Host Command Interface or the Host Command Server failed to read from the LU 6.2 connection that exists between it and the mainframe code. The process that detected the error will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 communications are configured properly.

`CWC0024I Control received value from mainframe signals termination.`

Explanation The Host Connection Interface or Host Command Server process received a code format value from the mainframe, indicating that termination was necessary. The detecting server process will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 communications are configured properly.

`CWC0025E Failure confirming` *`conversation`* `LU 6.2 conversation read.`

Where:

`conversation` is the inbound or outbound conversation.

Explanation The Host Command Interface or the Host Command Server failed to confirm that the conversation was read as requested by the mainframe program. The process that detected this failure will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 communications are configured properly.

`CWC0026E Failure sending over` *`conversation`* `LU 6.2 conversation.`

Where:

`conversation` is the inbound or outbound conversation.

Explanation The Host Command Interface or the Host Command Server detected a failure while attempting to send over the LU 6.2 conversation with the mainframe. The process that detected this failure will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 SNA profiles are configured properly.

`CWC0027E Failure closing` *`conversation`* `LU 6.2 conversation.`

Where:

`conversation` is the inbound or outbound conversation.

Explanation The Host Command Interface or the Host Command Server detected a failure while attempting to close the LU 6.2 conversation with the mainframe. The SNA host process that detected this failure will terminate.

Action Review any LU 6.2 communication errors generated in the mainframe's system log or the workstation's SNA stack error logs. Verify that your LU 6.2 SNA profiles are configured properly.

`CWC0028I` *`process`* `initialized successfully for domain` *`name`*`.`

Where:

`process` is the process.

`name` is the defined domain name.

Explanation A process has initialized successfully for the domain. The SNA host process will continue with execution.

Action No user action is required.

`CWC0029E` *`process`* `started with invalid argument count.`

Where:

`process` is the process.

Explanation A process was started with an incorrect number of command line arguments. The process will terminate.

Action Verify that you entered the correct options. If you have entered the correct options on the command line or in the */opt/CSCOcb/etc/runprocess* script. Use the **cwb tac** command and notify the Cisco TAC.

`CWC0030E Domain name must be passed in to the` *`process`*`.`

Where:

`process` is a process.

Explanation A process was started without the domain name passed as an argument. The process requires the domain name argument to determine the proper configuration file to use. The process will terminate.

This message is displayed if the **cwbhmond** process is not given a domain name on the command line as its first command argument.

Verify that the following UNIX files were not incorrectly modified:

- /opt/CSCOcb/etc/runprocess
- /opt/CSCOcb/etc/CWBlue.conf

`CWC0031E Invalid transaction program name executable used to start HCI.`

Explanation The Host Command Interface was started with an invalid transaction program name. The transaction program name did not have the domain name (for which the servers are being started) appended to the executable name. The process that detected this failure will terminate.

Action Verify that the following UNIX files were not incorrectly modified:

- /opt/CSCOcb/ect/runprocess
- /opt/CSCOcb/eetc/CWBlue.conf

`CWC0032E` *`process`* `encountered invalid value for configuration parameter` *`parameter_name`*

Where:

`process` is the process name.

`parameter_name` is the Maps SNA host configuration parameter.

Explanation An SNA host process was started but the specified configuration parameter is set incorrectly. The specified configuration parameter is critical to the operation of the process. The process that detected this failure will terminate.

Action Set the configuration parameter with the proper value and restart the process.

`CWC0033E` *`process`* `needs the` *`variable`* `environment variable set properly.`

Where:

`process` is the process.

`variable` is the environment variable.

Explanation A process was started without the environment variable set. The specified environment variable is critical to the operation of the process. The process that detected this failure will terminate.

Action Set the environment variable with the proper value and restart the process.

`CWC0035E` *`process`* `failed calling` *`function`*

Where:

`process` is the process or function.

`function` is the function.

Explanation A process or function has failed in its call to a function. In most cases the process or function will terminate.

Action Normally, more detailed error messages will accompany this message. Review all generated error messages in an effort to resolve the error.

`CWC0036E` *`process`* `failed calling` *`function`* `with rc:` *`rcnumber`*

Where:

`process` is the process or function.

`function` is the function.

`rcnumber` is the integer return code.

Explanation A process or function has failed in its call to a function and received a return code. In most cases, the process or function will terminate.

Action Normally, more detailed error messages will accompany this message. Review all generated error messages in an effort to resolve the error.

`CWC0037E` *`process`* `failed calling` *`function`*`, reason:` *`message`*

Where:

`process` is the process or function.

`function` is the function.

message is the text of the error message.

Explanation A process or function has failed in its call to a function and received an error message. Usually, the process or function will terminate.

Action Normally, more detailed error messages will accompany this message. Review all generated error messages.

CWC0038I *process* for domain *domain* will terminate after waiting for other processes to end.

Where:

process is the process or function.

domain is the domain name.

Explanation The listed process will terminate as soon as its dependent processes terminate. Normally other messages will accompany this message to explain why the process is ending.

Action No user action is required.

CWC0039W An instance of *process* for domain *domain* is already running.

Where:

process is the process or function.

domain is the domain name.

Explanation A process or function is already running for the domain. Perhaps you tried to start a daemon (such as *cwbhcid*, *cwbhcmdd*, or *cwbhmond*), but it is already running. The process will not be restarted.

Action No user action is required.

CWC0040E *process* failed to open file *path*, reason: *message*

Where:

process is the process or function.

path is the full file path, including the file name.

message is the text of the error message.

Explanation A process or function has failed to open a file and received an error message. The process that detected the error will terminate.

Action Check file permissions to ensure that the process has the ability to read and write to the file.

`CWC0041W Attempt to connect to` *process* `failed, retrying.`

Where:

process is the process or function.

Explanation An attempt to setup a socket connection to the specified daemon failed.

Action No action is necessary. An attempt to connect will be retried.

`CWC0042E Memory allocation failure, check available memory.`

Explanation A process attempted to obtain more memory from the operating system and failed. The process that detected the error will terminate.

Action Verify that available memory requirements on the workstation have not been exceeded.

`CWC0043E Unable to obtain host TCP/IP address from host name:` *host*`.`

Where:

host is the TCP/IP host name.

Explanation A process attempted to get the TCP/IP address for the TCP/IP host machine and failed. The process that detected the error will terminate.

Explanation If the machine uses the */etc/hosts* file to resolve TCP/IP addresses, make certain that the specified host name has an entry. If the machine uses a name server to resolve addresses, verify that the name server knows the host name.

`CWC0044W Waiting for previous instance of` *`process`* `for domain` *`domain`* `to end.`

Where:

`process` is the name of the process.

`domain` is the name of the domain.

Explanation A previous instance of the indicated daemon is still running.

Action No action is necessary.

`CWC0045E` *`process`* `for domain` *`domain`* `detected an unsupported mainframe version.`

Where:

`process` is the name of the process.

`domain` is the name of the domain.

Explanation The mainframe and workstation versions are not comparable.

Action Install the correct level of software on both the mainframe and workstation.

`CWC0046E` *`process`* `for domain` *`domain`* `failed to receive a response for the version request.`

Where:

`process` is the name of the process.

`domain` is the name of the domain.

Explanation The workstation did not receive a response from the mainframe for the version requested.

Action Ensure that the correct level of mainframe software is installed and running on the mainframe. You might need to adjust the mainframe command time out value (SVCMD_TIMEOUT).

`CWC0047E` *`process`* `for domain` *`domain`* `lost mainframe connection; will try to re-establish. Code` *`code`*.

Where:

`process` is the name of the process.

`domain` is the name of the domain.

`code` is the error code.

Explanation The workstation lost its connection to the mainframe.

Action No action is required. The workstation periodically will try to reestablish a connection to the mainframe.

`CWC0048I` *`process`* `process has exited.`

Where:

`process` is the process that exited.

Explanation A process has terminated.

Action Review any generated error messages to determine the cause of the process termination if the termination was abnormal.

`CWC0049I` *`process`* `process of domain` *`name`* `has exited.`

Where:

`process` is the process that exited.

`name` is the domain name.

A process of a domain has terminated.

For example, if the *cwbhmond* process fails to initiate a session with the Sybase application program interface (API), this error message is logged.

Action Review any generated error messages to determine the cause of the process termination if the termination was abnormal.

`CWC0050I` *`process`* `process of domain` *`name`* `has exited with code` *`code`*`.`

Where:

`process` is the process that exited.

`name` is the defined domain name.

`code` is the error code.

Explanation The named process has exited.

Action Review any generated error messages to determine the cause of the process termination if the termination was abnormal. If the program termination was not intended, examine these messages to resolve the problem.

`CWC0051W Status and/or Discover task not active on mainframe.`

Explanation The Status and Discovery subtasks on the mainframe are not running. No SNA correlation information is being sent from the mainframe.

Action Ensure that the mainframe STATUS and DISCOVERY subtasks are configured and active.

`CWC0052E Invalid buffer size for` *`process`* `message. Domain:` *`domain`*

Where:

`domain` is the domain name.

`message` is the message.

Explanation The named process has received a invalid buffer. The process will end.

Action Use the **cwb tac** command and notify the Cisco TAC.

`CWC0053E Invalid buffer structure. Domain: domain`

Where:

domain is the domain name.

Explanation An invalid buffer was received. The process will end.

Action Use the **cwb tac** command and notify the Cisco TAC.

`CWC0054W Connection to command server daemon failed for domain.`

Where:

domain is the domain name.

Explanation The Host Connection Interface was unable to connect to the Host Command Server.

Action Other messages might accompany this message. Attempt to resolve the problem based on these messages. Ensure that the product was properly installed and configured. If the error persists, use the **cwb tac** command and notify the Cisco TAC.

`CWC0055W Connection to Status Monitor daemon failed for domain domain.`

Where:

domain is the domain name.

Explanation The Host Connection interface was unable to connect to the Status Monitor.

Other messages might accompany this message. Attempt to resolve the problem based on these messages. Ensure that the product was properly installed and configured. If the error persists, use the **cwb tac** command and notify the Cisco TAC.

`CWC0056E Invalid message type received by` *`process1`* `from` *`process2`*`: type`

Where:

`process1 and process2` are processes.

`type` is the message type.

Explanation A process received an invalid message type from another process. The invalid message will be ignored, and processing will continue.

Action If this message persists, note the message contents, use the **cwb tac** command, and notify the Cisco TAC.

`CWC0057W Client is not currently registered, filter request rejected.`

Explanation A client process attempted to send a filter request to a server process to which the client process was not properly registered. The filter request was rejected for this reason by the server.

Action No user action is required.

`CWC0058W Client is not currently registered, command not submitted to mainframe.`

Explanation A client process attempted to send a mainframe command to the Host Command Server process to which the client process was not properly registered. Host Command Server will reject the client's mainframe command request.

Action No user action is required.

`CWC0059W Maximum number of clients already registered, request rejected.`

Explanation A client process attempted to register with a server process, but the server process already had the maximum number of 100 clients it was permitted to serve. The server process rejected the client's request.

Action No user action is required.

`CWC0060W Timed out waiting for server registration response.`

Explanation A client process issued a registration request to its server process and no registration response has been received by the client in the provided time. The client will either continue to wait or exit depending upon the user action chosen.

Action You can continue waiting for the registration response or exit the client process. Verify that the proper server process is active and that the configuration parameters for the appropriate domain are correct.

`CWC0061W Timed out waiting for command response from Command Server.`

Explanation A client process issued a registration request to the Host Command Server process and no registration response has been received by the client in the provided time. The client will either continue to wait or exit depending upon the user action chosen.

Action Verify that the Host Command Server (HCS) process on the workstation is active. If it is not active, start it. If it is active, re-issue the failing command.

`CWC0062E` *`process`* `error message:` *`message`*`.`

Where:

`process` is the server process that detected the error.

`message` is the text of the error message.

Explanation The server process detected a critical error and notified the client of the error.

Action Review the error message to determine the cause of the error and correct the problem.

`CWC0063E Verify that the HCI and Command Servers are active.`

Explanation The process has detected a possible problem with connection to the mainframe, indicating that the Host Command Interface and Host Command Server might have terminated.

Action Ensure that the Host Command Interface and Host Command Server are active and functioning properly. If they are not active, review all error messages and restart them once any problems have been corrected. If they are still active, attempt to rerun the failing process.

`CWC0064W Command not processed. Verify that the HCI and Command Servers are active.`

Explanation A mainframe command was issued but the mainframe application was unable to process it. The Host Command Interface or Host Command Server, or both might be no longer active or function properly. No further processing for the issued command will take place.

Action Verify that the Host Command Interface and Host Command Server are up and functioning properly. If they are not active, restart them. If they do not restart, use the **cwb tac** command and notify the Cisco TAC.

`CWC0065W Sybase database login failure.`

Explanation The workstation application could not log in to the CiscoWorks Blue database using the ID and password defined during configuration. Either Sybase is not running, or the ID and password are invalid.

Action Determine whether the database is running on the workstation. Determine whether the ID and password, defined during workstation configuration, are correct.

Troubleshooting the APPN/SNASw Application

This section describes some general APPN/SNASw troubleshooting procedures for initial problem resolution, and then lists specific symptoms and possible remedies.

General Troubleshooting

If the APPN/SNASw application fails to operate correctly, verify that the environment variables are set in the **cwbinit** script according to the values in Chapter 3, "Installing and Configuring CiscoWorks Blue."

Go to another view, then return to this view. If the problem has not cleared up, exit the application, remove the Map files again, and restart the application.

Diagnosing APPN/SNASw Symptoms

Table 11-1 lists symptoms that your APPN/SNASw application might demonstrate and refers you to some diagnostic techniques to resolve the problems.

Table 11-1 APPN/SNASw Troubleshooting Symptoms

For this symptom...	See this section...
Cannot find LU	LU Cannot Be Found, page 11-51
Global view is empty	Global Map Is Blank, page 11-51
Good connection displayed as degraded	Good Connection Appears Degraded, page 11-52
Incorrect status	Incorrect Status, page 11-52
Link station is not displayed	Link Station Does Not Appear, page 11-52
Network node status is unknown	Network Node Status Unknown, page 11-51

Global Map Is Blank

If the global map is blank, you might have one of the following problems:

- You specified an incorrect IP address or read community string in the startup dialog box.
- The IP path to the network topology agent is unavailable or degraded.
- The IP address and read community string you specified are not of an APPN/SNASw network node, or APPN/SNASw is not started on that node.

To resolve this problem, perform one or more of the following:

- Select **Administration > Discover All**.
- Use the **ping** command to verify operation of the network topology agent, or select **Tools > PathTool** from the menu bar to verify that it is accessible.
- Use the **telnet** command to access the agent and start the APPN/SNASw protocol.
- Stop and restart APPN/SNASw using a valid network topology agent.

Network Node Status Unknown

If the status of all network nodes is unknown to the application, the network topology agent could have failed, or APPN/SNASw could have been stopped in that device, or the SNMP request might have failed. Use the **ping** command or select **Tools > PathTool** from the menu bar to verify that the network topology agent is accessible. If necessary, use the **telnet** command to log in to the agent to start the APPN/SNASw protocol.

LU Cannot Be Found

If APPN/SNASw cannot find a known LU, use the following procedure:

Step 1 Select each node on the map, one at a time.

Step 2 At each node, click the right mouse button.

Step 3 Select **Get Directory** from the menu.

Step 4 Repeat Step 1 through Step 3 for the next node.

Link Station Does Not Appear

If a known link station does not appear in the **List TGs and Links** window, use the following procedure:

Step 1 Close the **List TGs and Links** window.

Step 2 Select the node on which the missing link is defined.

Step 3 Click the right mouse button.

Step 4 Select **Get Local Topology** from the menu.

Step 5 Reopen the **List TGs and Links** window to see if the link is listed. Or, set the *autolocaltopo* variable in the *cwbinit* file to ALL or NN_ONLY and restart the application.

Good Connection Appears Degraded

If a known good connection appears degraded (yellow), a defunct TG number might exist in the network topology agent's database. According to an APPN/SNASw algorithm, the network topology agent will delete the defunct number within a few days. When you start the APPN/SNASw application after that deletion occurs, the connection does not appear degraded.

Incorrect Status

If the status of a port, link, or transmission group is reported incorrectly, refresh the information by using the following procedure:

Step 1 On the map, select the owning node.

Step 2 Click the right mouse button.

Step 3 Select **Get Local Topology** from the menu.

APPN/SNASw Error Messages

The following error messages are unique to the APPN/SNASw application. They are displayed in the APPN/SNASw Motif message box and written to the message log.

```
Current view_name view type conflicts with reserved name prefix
of file.
Save map file filename Failed!
```

Where:

view_name is the name of the view that you are trying to save to a file.

- For APPN/SNASw the *view_name* can be Global, Local, or Port.
- For DLSW the *view_name* can be Global, Key Devices, Focus Peer, PU Dependency, or LU Dependency.
- For RSRB the *view_name* can be Global, Virtual Ring, Focus Peer, PU Dependency, or LU Dependency.

filename is the name of the file in which you are trying to save the view.

Explanation You tried to use **File > Save As** to save a map to a file, but the file prefix is one of the reserved Maps file prefixes. Maps reserves the following file prefixes:

- For APPN/SNASw: Local_, Port_
- For DLSW: Key_Devices_, Focus_
- For RSRB: VR_, Focus_
- For all: Global_, PU_, LU_

Action Do not use **File > Save As** to save to a file with one of the reserved prefixes.

`Database initialization failure`

Explanation
APPN/SNASw failed to connect to the network management system database before discovery.

Action
If you have HP OpenView or NetView installed, you can use the **ovstatus** command, which typically is located in the */usr/OV/bin* or */opt/OV/bin* directory. The **ovstatus** command displays the status of daemons and processes. Ensure that all network management daemons are running and restart those that are not running.

`Device name & read community required`

Explanation
APPN/SNASw must send an SNMP MIB request to a node, but no device name is known for this node.

Action
If the displayed default device name is not correct, enter the correct device name and read community string. Your input also establishes the default name for future SNMP MIB requests. If you do not know the device name, or if the node cannot be an SNMP agent, click **Cancel** to terminate the request.

`Invalid view type`

Explanation When switching views, for example from global view to focus view, a correct filename and format is read but the view type in the file is wrong. For example, the map is changing to a focus view, but the view type says it is a Virtual Ring view.

Action Delete or move the particular map file.

```
No devices discovered
```

Explanation
No devices were available to be discovered.

Action
Review the device list in the seed file or network management system database so that discovery has a chance of success. Then use **Administration** > **Discover** to retry the discovery, or exit the application and restart it. In the Startup Query window, specify a topology agent that is known to be reliable.

```
Reading map file filename. Incorrect format or version.
Open file Failed!
```

Where:

filename is the name of a map file.

Explanation You are reading a map file with an incorrect format or version. This error occurs when a map file format changes between versions of Maps and you attempt to read the incompatible format.

Action Delete or move the particular map file.

```
View could not be retrieved
```

Explanation
A map view requires data that is not available to the APPN/SNASw application. Typically, this happens when you request the ports and links view but local topology is not available from the target node.

Action
If the target node can act as a topology agent, and you know its IP address or its device name and read community string, select **Get Local Topology** from its popup menu. **Get Local Topology** collects the local topology.

`View may be incomplete`

Explanation

An **Adjacent Nodes** view is shown for a node that does not have local topology information available. Only adjacent nodes learned from the global view or from local topology collection from other nodes are displayed. Adjacent EN and LEN nodes are, most likely, not shown.

Action

If this node can act as an agent and you know its IP address or its device name and read community string, collect its local topology now.

`Will retry by polling`

Explanation

A network topology agent has been selected but is not returning network topology information. No global map is currently available. The application will retry this agent at the network topology polling rate.

Action

Perform the following steps in order. Stop when one is successful.

Step 1 Select **Administration > Discovery** to discover a new network topology agent.

Step 2 Ensure that the selected network topology agent is an APPN/SNASw network node with the APPN/SNASw MIB, and that the IP address or device name you specified is correct. If not, stop the APPN/SNASw application and restart it with a new network topology agent.

Step 3 Ensure that the APPN/SNASw protocol is active on the target agent.

Step 4 Use the **ping** command to see if the agent is alive and accessible.

Troubleshooting the Web Browser

This section presents troubleshooting techniques for the web browser.

Web Browser Fails

If your web browser cannot access the web server, try one of the following:

At the Web Server

If the web browser cannot access the web server, look at the web server's log files. The CiscoWorks Blue web server log files are */opt/CSCOcwbC/apache/var/log/access_log* and */opt/CSCOcwbC/apache/var/log/error_log on UNIX*. The *access_log* file lists all accesses to the web server. The *error_log* file lists individual errors in accessing the web server.

At the Web Browser

If selecting **Tools > Web Browser** from a Motif application fails, look at the */opt/CSCOcb/etc/runweb* file and ensure that the environment variables are set correctly for your directory structure. Verify that Netscape is installed. If you installed Netscape after you installed CiscoWorks Blue, Netscape must be in the PATH.

Also, you can try turning off proxy server use at the web browser. Check with your system administrator before you do this. To turn off proxy use for the Netscape browser, for example, select **Options > Network Preferences**. Select the **Proxies** tab, and click **No Proxies**. Click **OK** and try to access the web server again.

Cannot Access CiscoWorks Blue Web Pages

If you cannot access the CiscoWorks Blue web pages, use the Process Manager to ensure that the *CWBHTTPDAdapter* is running.

Unexpected Web Page Displayed

If you accessed the CiscoWorks Blue web server but saw some other page, this means another web server is already using port 80. For example, when you installed CiscoWorks Blue Maps, no other web server was running, so the CiscoWorks Blue web server was configured for port 80. But later, when you started the CiscoWorks Blue web server or tried to display the CiscoWorks Blue web page, some other web server was already using port 80. If you need to use a different port, you must reinstall the CiscoWorks Blue products.

Change the URL at the Browser

To specify port 8080 in the web browser, enter the following URL in the browser:

http://*workstation_name***:8080**

Where:

workstation_name is the name of the workstation where the Maps web server is installed.

Troubleshooting the HTML Online Help

If the online help for the web browser, the Administration program, the Process Manager, or the Message Logger does not launch successfully, edit the following files to ensure that the path to the Netscape executable is correct:

- /opt/CSCOcb/etc/runweb
- /opt/CSCOcwbC/classes/com/cisco/nm/cmf/kubit/process/displayMain.properties
- /opt/CSCOcwbC/classes/com/cisco/nm/cmf/kubit/logger/logger.properties

The installation program asks you for this path. If you enter the wrong path, the online HTML help might not work.

Controlling PU and LU Activation and Deactivation

This chapter provides information about activate and deactivating PUs and LUs by using the Maps Motif interface.

The chapter includes the following sections:

Using the Maps Motif interface, you can activate and deactivate PUs from the PU List window and you can activate and deactivate LUs from the LU List window. However, before you can activate or deactivate PUs or LUs, you must perform the following tasks:

- Set up the CiscoWorks Blue mainframe program, as described in the *CiscoWorks Blue Maps and SNA View Mainframe Installation Guide*.
- As root user, verify a special file called *SnaActDeactOn* is in the *$CWBROOT/etc* directory. If the file is removed or owned by a user other than root, you cannot activate and deactivate PUs and LUs.

Enabling SNA Activation and Deactivation

To enable SNA activation and deactivation, use the following procedure to create the *$CWBROOT/etc/SnaActDeactOn* file:

Step 1 Exit any Maps application by selecting **File > Exit Program** from the menu bar.

Step 2 Become the root user by entering the following command:

su root

Step 3 When prompted, enter the root user's password.

Step 4 Change to the *$CWBROOT/etc* directory by entering the following command:

cd /opt/CSCOcb/etc

Step 5 Create an SNA activation/deactivation file by entering the following command:

touch SnaActDeactOn

Step 6 Change back to your username by entering the following command:

exit

Step 7 Ensure that the mainframe SEC parameter card is set to **NO** in NSPPARM.

Step 8 Restart the application.

Disabling SNA Activation and Deactivation

To disable SNA activation and deactivation, use the following procedure to remove the *$CWBROOT/etc/SnaActDeactOn* file:

Step 1 If you are already running a Maps application, exit the application by selecting **File > Exit Program** from the menu bar.

Step 2 Become the root user by entering the following command:

su root

Step 3 When prompted, enter the root user's password.

Step 4 Change from the current directory to the *$CWBROOT/etc* directory by entering the following command:

cd /*opt/CSCOcb*/**etc**

Step 5 Remove the SNA activation/deactivation file with the following command:

rm SnaActDeactOn

Step 6 Switch back to your username by entering the following command:

exit

Step 7 Restart the application.

Mounting a CD-ROM on UNIX Workstations

This appendix provide instructions on how to mount a CD-ROM from a local or remote system so you that can install and configure CiscoWorks Blue Maps or CiscoWorks Blue SNA View on a workstation.

Also, this appendix covers how to export the CD-ROM from a remote workstation and then mount it on the local workstation.

This appendix contains the following main sections:

Mounting from a Local or Remote CD-ROM Drive on HP-UX and Solaris Systems

You can install CiscoWorks Blue Maps and SNA View from a CD-ROM drive attached to your system or from a drive connected to a remote system. You must first mount the local or remote device on the local system.

Caution Avoid exposing the CD-ROM to direct sunlight because it could harm the contents.

To install from a CD-ROM, perform the following tasks:

- Export the CD-ROM file system from a remote workstation.
- Mount the CD-ROM from your local workstation.

Exporting a CD-ROM File System from a Remote HP or Solaris System

This section covers how to export a CD-ROM file system from a remote system.

Caution The instructions for mounting a remotely exported CD-ROM drive on a local system are for *like* systems. For example, the instructions are for exporting a CD-ROM file system from an HP-UX system and mounting it on another HP-UX system for installation, or for exporting from a Solaris system and mounting on Solaris, but not for cross-platform operation. If necessary, your system administrator can help you with cross-platform exporting and mounting.

To export a CD-ROM file system, perform the following steps on the remote system:

Step 1 Insert the CD-ROM in the CD-ROM drive.

Step 2 Log in as the root user.

Step 3 If the */cdrom* directory already exists, proceed to the next step. If the */cdrom* directory does not exist, create it with the **mkdir** command:

```
mkdir /cdrom
```

Step 4 If an exports file does not exist, create one using a text editor.

- For Solaris, the file is */etc/dfs/dfstab.*
- For HP-UX, the file is */etc/exports.*

Step 5 Edit the exports file to include this line:

/cdrom -ro

Step 6 If you just created a new exports file (*/etc/dfs/dfstab* or */etc/exports*) in Step 4, you must now enable your workstation as a Network File System (NFS) server. To start the *nfsd* server, enter the following commands:

- On Solaris

  /etc/init.d/nfs.server start

- On HP-UX

  /sbin/init.d/nfs.server start

  /usr/sbin/rpc.mountd -n

Step 7 On Solaris only, add the following line to the *etc/dfs/dfstab* file:

share -F nfs -o -ro /cdrom/cdrom0

Step 8 Mount the CD-ROM.

- On Solaris

  The **vold** server automatically manages the CD-ROM device and performs the mounting. The CD-ROM may automatically mount onto the */cdrom/cdrom0* directory. If you are running File Manager, a separate File Manager window displays the contents of the CD-ROM disk. If the */cdrom/cdrom0* directory is empty because the CD was not mounted, or if the File Manager did not open a window showing the contents of the CD-ROM disk, verify the **vold** server is running by entering the following sequence of commands:

  ps -ef | grep vold | grep -v grep

  If the system does not display anything, restart the server:

  /usr/sbin/vold &

  If the **vold** server is running but did not mount the CD, stop the **vold** server process and then restart it:

kill -15 *process_ID*

/usr/sbin/vold &

Where:

process_ID is the UNIX process ID of the **vold** server.

Then enter the mount command:

/usr/sbin/mount -r /dev/sr0 /cdrom

- On HP-UX

  Use the following commands to mount the CD-ROM:

  /etc/mount -o ro -t cdfs /dev/*device_filename* **/cdrom**

  Where:

  -o ro mounts the CD-ROM in read-only mode.

  -t indicates the type of file system: **hsfs** for the ISO 9660 standard, or **cdfs** for the High Sierra standard with Rock Ridge extensions.

  device_filename is the name of the device you want to mount (for example **/dev/dsk/c201d2s0***)* or a different device name reported by the **/etc/ioscan** program for the CD-ROM device.

Step 9 If the */etc/exports* file existed previously, enter the following command to run exportfs:

exportfs -va

If */etc/exports* did not exist previously, reboot your system.

reboot

Continue to the "Mounting a Remotely Exported CD-ROM File System on a Local HP or Solaris System" section on page B-5.

Mounting a Remotely Exported CD-ROM File System on a Local HP or Solaris System

To mount a file system that is exported from a remote system, perform the following steps on the local system:

Step 1 Log in as the root user.

Step 2 If a */cdrom* directory does not already exist, create it by entering the **mkdir** command:

mkdir /cdrom

Step 3 To mount a file system that is exported from a remote system, use the mount command as shown below.

mount *remote_hostname*:*remote_filesystem local_mount_point*

Where:

remote_hostname is the name of the remote workstation.

remote_filesystem is the name of the file system on the remote workstation.

local_mount_point is the name to be used on the local workstation.

For example, to mount the */cdrom* file system from a remote host called *faraway* on a local directory named */cdrom*, you would use the following command:

mount faraway:/cdrom /cdrom

The remote CD-ROM is ready for software installation on the local system.

Mounting a Local CD-ROM on HP-UX or Solaris

To prepare the system for software installation from a local CD-ROM drive, complete the following steps:

Step 1 Insert the CD-ROM in the CD-ROM drive.

Step 2 Log in as the root user.

Step 3 If the */cdrom dir*ectory already exists, proceed to the next step.

If a */cdrom* directory does not exist, create it with the **mkdir** command:

mkdir /cdrom

Mount the CD-ROM.

- On Solaris

  The **vold** server automatically manages the CD-ROM device and performs the mounting. The CD-ROM may automatically mount onto the */cdrom/cdrom0* directory. If you are running File Manager, a separate File Manager window displays the contents of the CD-ROM disk. If the */cdrom/cdrom0* directory is empty because the CD was not mounted, or if File Manager did not open a window displaying the contents of the CD-ROM disk, verify that the **vold** server is running by entering the following sequence of commands:

  ps -ef | grep vold | grep -v grep

  If the system does not display anything, restart the **vold** server using the following command:

  /usr/sbin/vold &

  If the **vold** server is running but did not mount the CD-ROM, stop and restart the **vold** server process:

  kill -15 *process_ID*

  /usr/sbin/vold &

  Where

  process_ID is the UNIX process ID of the **vold** server.

- On HP-UX

  /etc/mount -o ro -t cdfs /dev/*device_filename* **/cdrom**

  Where:

  -o ro mounts the CD-ROM in read-only mode.

-t indicates the type of file system: **hsfs** for the ISO 9660 standard, and **cdfs** for the High Sierra standard with Rock Ridge extensions.

device_filename is the name of the device you want to mount (for example **/dev/dsk/c201d2s0***)* or a different device name reported by the **/etc/ioscan** program for the CD-ROM device.

Mounting from a Local or Remote CD-ROM Drive on AIX Systems

You can install CiscoWorks Blue Maps from a CD-ROM drive attached to your system or from a drive connected to a remote system. You must first use SMIT to mount the local or remote device on the local AIX system.

Caution Avoid exposing the CiscoWorks Blue Maps CD-ROM to direct sunlight because it could harm the contents.

To install Maps on AIX from a CD-ROM, you can do one of the following:

- Mount the CD-ROM from a remote workstation.
- Mount the CD-ROM from your local workstation.

Mounting from a CD-ROM Drive on the Local AIX Workstation

This section describes how to mount the CD-ROM drive from the local workstation. If you have already performed this procedure, or if another device is already mounted on the mount point, this process will fail.

If you are using SMIT from a remote workstation, be sure to export the DISPLAY variable to your workstation before starting SMIT. Otherwise, you will be using SMITTY.

To mount the CD-ROM on the file system from a local CD-ROM drive, use SMIT to perform the following steps:

Step 1 Insert the Maps CD-ROM into the CD-ROM drive.

Step 2 Log in as the root user.

Step 3 Enter the following **smit** command:

```
# smit
```

Step 4 From the System Management menu, click **System Storage Management (Physical & Logical Storage)**.

Step 5 Select **File Systems**.

Step 6 Select **Add/Change/Show/Delete File Systems**.

Step 7 Select **CDROM File Systems**.

Step 8 Select **Add a CDROM File System**.

Step 9 Click the "DEVICE name" **List** button and select the device name (such as */dev/cd0*) from the list that appears.

Step 10 In the Mount point field, enter the name of a mount point directory (such as */cdrom*).

Step 11 Click **OK** and read the output.

Step 12 Click **Done**.

Step 13 Terminate SMIT by selecting **Exit SMIT** from the Exit menu.

Step 14 Use the **mountfs** command to mount the file system:

```
smit mountfs
```

Step 15 Click the "FILE SYSTEM name" **List** button, and select a device name (such as */dev/cd0*) from the list that appears.

Step 16 In the "DIRECTORY field," enter the name of a mount point directory (such as */cdrom*).

Step 17 Click the "TYPE of file system" **List** button, and select **cdrfs** as the file system type.

Step 18 Set the "Mount as Read-Only System" field to **yes**.

Step 19 Click **OK** and read the output, and then click **Done**.

Terminate SMIT by selecting **Exit SMIT** from the Exit menu.

Mounting from a CD-ROM Drive on a Remote AIX Workstation

This section covers how to mount a remote CD-ROM on your local workstation. Installation of CiscoWorks Blue Maps does not require any disk space on the remote system. The software is copied across the network to the local workstation.

On the Remote System

To mount the CD-ROM on the local file system from a remote CD-ROM drive, first mount the CD-ROM on the remote system using the following procedure. If you have already performed this procedure, or if another device is already mounted on the mount point, this process will fail.

Step 1 Insert the Maps CD-ROM into the CD-ROM drive.

Step 2 Log in as the root user.

Step 3 To start SMIT, enter the **smit** command:

```
# smit
```

Step 4 On the System Management list, select **System Storage Management (Physical & Logical Storage)**.

Step 5 Select **File Systems**.

Step 6 Select **Add/Change/Show Delete File Systems**.

Step 7 Select **CDROM File Systems**.

Step 8 Select **Add a CDROM File System**.

Step 9 Click the "DEVICE name" **List** button, and select the device name (such as */dev/cd0*) from the list that appears.

Step 10 In the "Mount point field," enter the name of a mount point directory (such as */cdrom*).

Step 11 Click **OK** and read the output.

Step 12 Click **Done**.

Step 13 Terminate SMIT by selecting **Exit SMIT** from the Exit menu.

Step 14 Use the **mountfs** command to mount the file system:

```
# smit mountfs
```

Step 15 Click the "FILE SYSTEM name" **List** button and select a device name (such as */dev/cd0*) from the list that appears.

Step 16 In the "DIRECTORY field," enter the name of a mount point directory (such as */cdrom*).

Step 17 Click the "TYPE of file system" **LIST** button and select **cdrfs** as the file system type.

Step 18 Set the "Mount as Read-Only System" field to **yes**.

Step 19 Click **OK** and read the output, and then click **Done**.

Step 20 Terminate SMIT by selecting **Exit SMIT** on the Exit menu.

Step 21 Enter the following command at the system prompt:

```
# smit mknfsexp
```

Step 22 In the "PATHNAME of directory to export" field, enter the path name (such as */cdrom*).

Step 23 Use the arrow keys to change the "Mode to Export Directory" field to **read-only**.

Step 24 Enter the appropriate information, if necessary, into any of the other fields.

Step 25 Click **OK**, read the output, then click **Done**.

Step 26 Terminate SMIT by selecting **Exit SMIT** from the Exit menu.

Mount the CD-ROM On the Local System

Perform the following steps on the local system to mount the remote file system.

Step 1 Enter the **smit** command:

```
# smit mountfs
```

Step 2 In the "FILE SYSTEM name" field, enter the device name from the remote system (such as */cdrom*).

Step 3 In the "DIRECTORY over which to mount" field, enter the name of the mount point directory (such as */cdrom*).

Step 4 Click the "TYPE of file system" **List** button and select **nfs** as the file system type.

Step 5 In the "REMOTE NODE" field, enter the name of the remote host, such as **host1.cisco.com**.

Step 6 Set the "Mount as Read-Only System" field to **yes**.

Step 7 Click **OK** and read the output, and then click **Done**.

Step 8 Terminate SMIT by selecting **Exit SMIT** on the Exit menu.

The CD-ROM is ready for software installation.

Unmounting the CD-ROM

Unmount the CD by logging in as the root user and entering the following commands at the local or remote workstation on which the CD-ROM is mounted:

cd /

umount */cdrom*

The CD-ROM device is unmounted from the */cdrom* directory. Remove the CD-ROM from the drive.

Database Tables

This appendix summarizes the database tables used by CiscoWorks Blue Maps and SNA View applications.

This chapter includes the following main sections:

Caution Do not modify database table information. On UNIX workstations, database-knowledgeable users should see the schema files located in */opt/CSCOcb/etc*.

Common Tables Used for the RSRB, DLSw, and VTAM Protocols

This section contains database tables used for the RSRB, DLSw, and VTAM. The database tables discussed in this section are found in *$CWBROOT/etc/AsaSchemaCommon*.

This section includes the following tables:

- Client List Table
- Devices Table
- Interface Table
- IP Address Table
- Locate Router Table
- Logical Views Table
- Membership Table
- MIB Version Table
- Node Table
- Physical Unit Table
- PU Dependents Table
- Process Control Table
- Ring Bridge Table

Client List Table

The Client List table (client_list) contains a list of graphical user interface (GUI) applications, which are registered with the monitor daemon so that views can be updated. There is one record for each client. The monitor daemon initializes its client list by reading entries from this table at startup; it updates the table by adding an entry for each registration request received and by deleting an entry for each deregistration request received. To clear the client list, start the monitor daemon with the **-c** option or edit this table to remove client records.

Devices Table

The Devices table (devices) stores necessary information about known devices. There is one record for each device. When the status field changes or when a device is added or removed, the display is updated.

Interface Table

The Interface table (if_table) is used to store information about the interface, such as the device ID, type, and physical address.

IP Address Table

The IP Address table (ipaddr_table) is used to store all of the IP addresses configured on each router. This table is used to correlate the IP addresses of all the routers obtained from the seed file or network management system database. Maps uses this table to show only one icon for each router although more than one alias might be entered in the Maps application.

Locate Router Table

The Locate Router table (locate_rtr_table) is used to generate the unique device ID for each new device. An entry is made in this table the first time the device is discovered.

Logical Views Table

The Logical Views table (logical_views) associates a sequence number with each type of view. This sequence number is passed to the GUI with every view. Sequence numbers are updated by several triggers set on devices and peer tables. When an alteration causes the view to change in any of those tables, the sequence number is incremented. By checking the sequence number, the GUI determines whether a view is up-to-date.

Membership Table

The Membership table (members) maintains a list of all devices connected or attached to a real or virtual ring. This table is used for displaying views centered on virtual rings and in determining which real rings are associated with each of the routers in the view.

MIB Version Table

The MIB Version table (mib_version) lists the version of each MIB for each protocol.

Node Table

The Node table (node_table) contains information about all the major nodes discovered by the SNA Host component. There is one record for each major node in this table.

Physical Unit Table

The Physical Unit table (pu_table) contains information about all discovered PUs. This table is initially populated by the SNA Host discovery process, but is constantly updated by the Status Monitor. For each PU, this table contains the PU name, MAC address, routing information field (RIF) (if available), PU type, local and remote MAC addresses, local and remote SAPs, and current status.

PU Dependents Table

The PU Dependents table (pu_dependents) contains information, taken from the RIF data, about the path a PU session takes through the network. There is one record for each device in the path. Each record contains the PU name of the device, the device type, and the device name.

Process Control Table

The Process Control table (process_control) contains entries for processes that can automatically restart.

Ring Bridge Table

The Ring Bridge table (ring_bridge) maintains information about the relationships between real rings and virtual rings on every known RSRB or DLSw device. This table maps directly to the (ring, bridge, ring) tuples extracted from the RIF of each device. Given a (ring, bridge, ring) tuple, Maps can determine the referenced device. Maps parses the PU's RIF to extract (ring, bridge, ring) tuples. And by referring to this tuple, Maps can determine the dependency list for the PU.

Typically, one virtual ring is defined per router, so this table has no more entries than the number of real Token Ring interfaces on the router. In terms of router configuration commands, every occurrence of the following router command results in one entry in the Ring Bridge table:

`source-bridge` *`real-ring`* `bridge-no` *`virtual-ring`*

The total number of entries in this table is an indication of the number of Token Rings in the network that are bridged using RSRB or DLSw.

Tables Used for the RSRB Protocol

This section covers the database tables used for the RSRB protocol. The database tables in this section are found in *$CWBROOT/etc/AsaSchemaRsrb.*

This section includes the following tables:

- Address ID Table
- Peer Table

Address ID Table

The Address ID table (addr_id) maps the IP address used for RSRB to the device ID. Typically, there is one IP address per device for RSRB, but there can be multiple IP addresses if the router defines more than one virtual ring. This table is used to establish peer relationships between routers by matching IP addresses in the Peer table.

Peer Table

The Peer table (peer_table) contains information about RSRB peers defined on every device. There is one record per peer definition per router. The poller constantly updates the status of the peers in this table. There are triggers for additions and deletions to this table.

Tables Used for the DLSw Protocol

This section covers the database tables used just by the DLSw Maps application. The database tables in this section are found in *$CWBROOT/etc/AsaSchemaDlsw*. This section includes the following tables:

- DLSw Address Table
- DLSw Circuit Table
- DLSw Peer Table

DLSw Address Table

The DLSw Address table (dlsw_addr_id) correlates each device ID with an IP address.

DLSw Circuit Table

The DLSw Circuit table (dlsw_circuits) stores the circuit information.

DLSw Peer Table

The DLSw Peer table (dlsw_peers) stores information about the DLSw peer device, such as the device ID, domain, local and remote address, and status of the peer connection.

CiscoWorks Blue Commands and Processes

This appendix provides a list of the commands and processes used by CiscoWorks Blue Maps and SNA View and contains the following main sections:

Audit Trail for cwb Commands

An audit trail can be created for logging all CiscoWorks Blue commands. The audit trail can be useful for diagnosing problems encountered while running CiscoWorks Blue. The audit trail is automatically saved in /opt/CSCOcb/logs/cwbcmd.log.

Database and Log File Maintenance

Database maintenance is performed using the **cwb maintenance** command. The **cwb maintentance** command is used to perform the following functions:

- Stop CiscoWorks Blue processes so that the database can be backed up safely.
- Back up the database file and database log
- Back up the apache and **cwb** command log files and clear the current logs to control the size of the log file.
- Start CiscoWorks Blue processes.

Using the cwb maintenance start Command

The **cwb maintenance start** command schedules a cron job to perform the maintenance processing. The schedule is set according to the HOUR, MINUTE, DATE, MONTH, and DAY parameters in the cwbinit file. Note that CiscoWorks Blue processes will be stopped while maintenance is done, and restarted afterwards.

The **cwb maintenance stop** command removes the cron job so that the CiscoWorks Blue maintenance will no longer run as scheduled.

The /opt/CSCOcb/etc/cwbinit file has been modified so that the scheduling of the cron job can be scheduled.

Setting the CiscoWorks Blue Maintenance Schedule

The options described in this section specify the time and frequency that automatic maintenance will be initiated through a cron job. To enable the scheduling, enter the **/opt/CSCOcb/bin/cwb maintenance start** command. You will be prompted to specify the times for the cron job to run

Table 0-1 Maintenance Schedule Options

Field	Value
HOUR	0 to 23
MINUTE	0 to 59

Table 0-1 Maintenance Schedule Options

Field	Value
DATE	1 to 31
MONTH	1 to 12
DAY	0 to 6 for Monday through Saturday, respectively; * for Sunday

The following excerpt from the cwbinit file shows possible settings for the maintenance schedule.

```
# ***************************************************
# CiscoWorks Blue Maintenance schedule setting
# ***************************************************

# The following set of options specify the time and frequency that
# automatic maintenance will be done via a cron job.  To enable this,
# you must run the command '/opt/CSCOcb/bin/cwb maintenance start'.
# HOUR, MINUTE, DATE, MONTH and DAY.
# The valid value for HOUR is 0 to 23.
# The valid value for MINUTE is 0 to 59.
# The valid value for DATE is 1 to 31 and *.
# The valid value for MONTH is 1 to 12 and *.
# The valid value for DAY is 0 to 6 and *. 0 = Sunday
#
# The following are several examples of value you can use to set the
# maintenance schedule.
#
# 1. every day at 12:00 AM (Midnight).
#    HOUR = 0
#    MINUTE = 0
#    DATE = *
#    MONTH = *
#    DAY = *
# 2. weekly on Saturday at 11:30 PM.
#    HOUR = 23
#    MINUTE = 30
#    DATE = *
#    MONTH = *
#    DAY = 6
# 3. monthly on the 28th at 6:00 AM
#    HOUR = 6
#    MINUTE = 0
#    DATE = 28
#    MONTH = *
#    DAY = *
# 4. Annually on 31st of Dec at 11:45PM
#    HOUR = 23
#    MINUTE = 45
#    DATE = 31
#    MONTH = 12
#    DAY = *
#
```

```
# The default value set here will run the maintenance every Sunday at
12:00 AM
# (Midnight).
HOUR = 0
MINUTE = 0
DATE = *
MONTH = *
DAY = 0
```

DLSw and RSRB Daemons

The core of the DLSw and RSRB applications is a set of daemons and database tables.

This section discusses the following information about daemons:

- Name of daemon
- Starting and stopping daemons
- Role of daemons in the operation of DLSw and RSRB Maps applications

The daemon names are shown in Figure D-1.

Figure D-1 Daemon Names

Daemon Name	Description
cwbmonitord	DLSw and RSRB monitor daemon.
cwbdlswpollerd	DLSw poller daemon.
cwbrsrbpollerd	RSRB poller daemon.
cwbtrapd	DLSw and RSRB trap daemon.

Stopping and Starting DLSw and RSRB Daemons

You can start and stop each daemon using the Process Manager, as described in Chapter 5, "Using the Process Manager" or with the following **cwb start** command:

cd /opt/CSCOcb/bin

cwb start *maps_daemon_command*

Where:

maps_daemon_command is a Maps daemon startup command for each Maps daemon, as shown in the following sections.

Usage Guidelines

- Only one copy at a time of any specific daemon can be run on the same workstation.
- A daemon can be stopped and restarted only by a user who has the correct permissions.
- Cisco recommends using the Process Manager to start and stop daemons.

Daemons Common to DLSw and RSRB

This section describes how to control daemons that are common to both DLSw and RSRB. This section covers the following daemons:

- cwbmonitord, page D-7
- cwbtrapd, page D-9

cwbmonitord

The monitor daemon (cwbmonitord**)** sends an update to the graphical map when it detects a change in the database. Primarily, the monitor daemon relies on the poller daemon and the trap daemon to update the database. The monitor daemon must be running for changes to appear on the graphical map.

The monitor daemon saves the list of GUI clients in the database. For example, RSRB and DLSW. When the monitor daemon is reset, it sends updates to the applications in this list.

cwb {start | stop} cwbmonitord

Syntax Description

-h	Displays a help message.
-v	Displays the version.
-c	Starts with an empty client list. Without this option, the monitor daemon reestablishes the list of GUI application clients that were registered when it was last run. See the "Client List Table" section on page C-2.
-t *sleep_time*	Specifies the number of seconds the daemon waits from when it completes one cycle until it starts the next cycle.
UDPport	Specifies the User Datagram Protocol port to which the monitor daemon listens for communication from the GUI client applications. The default is port 6000. If you want the monitor daemon to listen to a different port number, enter that number here. If you change the port number here, you must also change it in the **runprocess** script.

Defaults

If you start the monitor daemon with no options, it starts with default options using port 6000.

Usage Guidelines

You can stop the monitor daemon to avoid automatic updates to displayed graphical maps.

Use the **cwb start** and **cwb stop** commands to start and stop the monitor daemon.

cwbtrapd

The trap daemon (cwbtrapd) registers with the network management system's trap process to receive unsolicited status messages from routers. It should run at all times unless the routers are not configured to send traps. When a device generates a trap, the trap daemon updates device information in the database. It will also resend DLSw and APPN/SNASw traps back to the NMS in a human readable format. See (the Event Notification section) for more details

cwb start cwbtrapd [**-h** | **-v**]

cwb stop cwbtrapd

The trap daemon reports changes to the following states:

- RSRB Peer state
- DLSw Peer state
- DLSw Circuit state

Syntax Description

-h	Displays a help message.
-v	Displays the version.

Defaults

If you start the trap daemon with no options, it starts with default options.

RSRB Daemons

This section describes the RSRB daemons in the following subsections:

- cwbrsrbpollerd, page D-10
- Poller MIB Variables, page D-11

cwbrsrbpollerd

To continuously poll the MIBs in discovered routers for their ever-changing status, use the RSRB poller daemon **cwbrsrbpollerd** command.

cwb start cwbrsrbpollerd [-h | -v] [*PollerSleepTime***]**

cwb stop cwbrsrbpollerd

Syntax Description.

-h	Displays a help message.
-v	Displays the version.
PollerSleepTime	Specifies a slow polling timer value, which is the number of seconds the daemon can wait from when it completes one cycle until it starts the next cycle. The default PollerSleepTime is 600 seconds.

Defaults

The default PollerSleepTime is 600 seconds.

Usage Guidelines

If you start the poller daemon with no options, it starts with default options.

Use the **cwb start** and **cwb stop** commands to start and stop the RSRB poller daemon.

Poller MIB Variables

The poller daemon queries the following MIB variables in known RSRB-enabled devices (those in the Devices table that are flagged “discovered”):

- rsrbRemotePeerEncapsulation
- rsrbRemotePeerIPAddr
- rsrbRemotePeerState

If a known RSRB-enabled (discovered) device does not respond to the poller’s SNMP query, the poller daemon sets that device status to “Inactive.” If the device responds with its current Peer table, the Peer table is updated in the database. The monitor daemon monitors the database and sends any changes to the GUI applications.

DLSw Daemons

This section describes the DLSw daemons and contains the following subsections:

cwbdlswpollerd

To continuously poll the MIBs in discovered routers for their status, use the DLSw poller daemon **cwbdlswpollerd** command.

cwb start cwbdlswpollerd [-h | -v] [-P *PollingSleepTime***]**
[-C *PollingSleepTime***] [***PollingSleepTime***]**

cwb stop cwbdlswpollerd

Syntax Description.

-h	Displays a help message.
-v	Displays the version.
-P *PollingSleepTime*	Specifies the non-key-peer polling timer value in seconds; the number of seconds the poller waits from when it completes one cycle until it starts the next cycle. The **-P** option starts the poller daemon for non-key-peer polling and sets the sleep-time value. If you omit the **-P** *PollingSleepTime* value, the default is 600 seconds.
-C *PollingSleepTime*	Specifies the key-circuit polling timer value, in seconds; the number of seconds the poller waits from when it completes one cycle until it starts the next cycle. The **-C** option starts the poller daemon for circuit polling and sets the sleep-time value. If you omit the **-C** *PollingSleepTime* value, the default is 1200 seconds.
PollingSleepTime	This option starts the poller daemon for key-peer polling and sets the sleep-time value. If you omit the *PollingSleepTime* value, the default is 600 seconds.

Defaults

If you start the poller daemon with no options, it starts with default options.

Usage Guidelines

Use the **cwb start** and **cwb stop** commands to start and stop the DSLw poller daemon.

DLSw MIB Variables Queried During Polling

During DLSw polling, the poller queries the MIB that was discovered for DLSw. If the Cisco IOS release changed so that MIB support was changed, you must rediscover this device.

The following DLSw MIB variables are queried during polling:

DLSW-MIB (RFC 2024)	CISCO-DLSW-MIB
dlswNodeUpTime	ciscoDlswUpTime
dlswTConnOperLocalTAddr	ciscoDlswTConnOperLocalTAddr
dlswTConnOperConnectTime	ciscoDlswTConnOperConnectTime
dlswTConnOperState	ciscoDlswTConnOperState
dlswCircuitS1DlcType	ciscoDlswCircuitS1DlcType
dlswCircuitS1RouteInfo	ciscoDlswCircuitS1RouteInfo
dlswCircuitS2TDomain	ciscoDlswCircuitS2TDomain
dlswCircuitS2TAddress	ciscoDlswCircuitS2TAddress
dlswCircuitState	ciscoDlswCircuitState

Setting DLSw Poller Timers

You can configure the DLSw application to poll DLSw routers for peer information and for circuit information at different intervals. For information about polling intervals, see the section “Using the CWBINIT Preferences File” in the *CiscoWorks Blue Maps and SNA View User Guide*.

You can set the following polling intervals.

- Key-Peer polling polls just key routers for peer connection information. Peer polling looks for a router state change and a peer-connection state change.
- Non-Key-Peer polling polls just the non-key routers for peer connection information. Peer polling looks for a router state change and a peer-connection state change.
- Key-Circuit polling polls the key routers for circuit information. Circuit polling looks for a router becoming unreachable, a new or lost circuit, and a circuit state change.

When you start the poller daemon from the command line, you can start the following polling timers by specifying them in the runprocess script, as described in the "Changing Parameters on Process Calls" section on page D-49.

- **-P** *PollingSleepTime* starts the poller daemon for non-key-peer polling and sets the sleep-time value. If you omit the **P** *PollingSleepTime* value, the default is 600 seconds.
- **-C** *PollingSleepTime* starts the poller daemon for key-circuit polling and sets the sleep-time value. If you omit the **-C** *PollingSleepTime* value, the default is 1200 seconds.
- *PollingSleepTime* starts the poller daemon for key-peer polling and sets the sleep-time value. If you omit the *PollingSleepTime* value, the default is 600 seconds.

The sleep-time values determine how many seconds the poller daemon waits after polling is complete before it starts polling again.

Note If you start the poller daemon from the command line and specify just the **-C** polling option, the poller does only key-circuit polling. It does not perform peer polling.

APPN/SNASw Polling

The polling of APPN/SNASw devices is performed as a thread of *cwbsnamapsd*. If the APPN/SNASw protocol is not configured, APPN/SNASw polling is not performed.

APPN MIB Variables Queried During Polling

During APPN polling, the poller queries the MIB that was discovered for APPN. If the Cisco IOS release changed so that MIB support was changed, you must rediscover this device. The following APPN-MIB variables are queried during polling:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnNodeCpName	ibmappnNodeCpName
appnNodeType	ibmappnNodeType
appnLocalTgOperational	ibmappnLocalTgOperational
appnLocalTgCpCpSession	

The process next queries the following variables from the DLUR MIB:

DLUR-MIB (RFC2232)	OLD-DLUR-MIB
dlurDlusSessnStatus	dlurDlusSessnStatus
	dlurDlusName

If the **appn_pu_polling** parameter in *cwbinit* is set to **ON**, the following DLUR-MIB *(RFC 2232)* variables are also polled*:*

DLUR-MIB (RFC2232)	OLD-DLUR-MIB
dlurPuSscpSuppliedName	dlurPuName
dlurPuStatus	dlurPuStatus
dlurPuActiveDlusName	dlurPuActiveDlusName

If **appn_port_polling** parameter in *cwbinit* is set to **ON**, the following APPN-MIB variables are also polled:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnPortOperState	ibmappnNodePortState

If **appn_link_polling** parameter in *cwbinit* is set to **ON**, the following APPN-MIB variables are also polled:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnLsOperState	ibmappnNodeLsState
appnLsAdjCpName	ibmappnNodeLsCpName
appnLsTgNum	ibmappnNodeLsTgNum

First Time Polling

The first time a device is polled, the following APPN MIB variables are also polled:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnLocalTgDestVirtual	ibmappnLocalTgDestVirtual
appnNodeBrNn	ibmappnLocalTgCpCpSession

If **appn_port_polling** parameter in *cwbinit* is set to **ON**, the following APPN MIB variables are also polled the first time:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnPortDlcType	ibmappnNodePortDlcType
appnVrnPortName	

If **appn_link_polling** parameter in *cwbinit* is set to **ON**, the following APPN MIB variables are also polled the first time:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnLsPortName	ibmappnNodeLsPortName
appnLsCpCpSessionSupport	ibmappnNodeLsCpCpSession
	ibmappnNodeLsDlcType

Network Topology Polling

For network topology polling, the following IBM-6611-APPN-MIB variables are polled initially and as changes are detected (APPN-MIB variables are not queried during network topology polling):

ibmappnNnNodeFRName	ibmappnNnNodeFRFrsn
ibmappnNnNodeFRType	ibmappnNnNodeFRCongested
ibmappnNnNodeFRQuiescing	ibmappnNnTgFROwner
ibmappnNnTgFRDest	ibmappnNnTgFRNum
ibmappnNnTgFRFrsn	ibmappnNnTgFRDestVirtual
ibmappnNnTgFROperational	ibmappnNnTgFRCpCpSession

For network topology polling, the following IBM-6611-APPN-MIB variables are polled at each poll interval to detect changes in network topology (APPN-MIB variables are not queried during network topology polling):

ibmappnNodeUpTime	ibmappnNodeNnFrsn

If changes are detected, the initial variables are polled for the changed resources.

Host Connection Daemons

This section describes the host connection daemons used to process messages and commands between the workstation and the SNA mainframe computer. This section covers the following daemons:

- cwbhcid, page D-18
- cwbhcmdd, page D-19
- cwbhmond, page D-20

cwbhcid

The Host Connection Interface daemon (cwbhcid) runs in the workstation to control all communications with the SNA mainframe component. It gets messages from the mainframe, sends commands to the mainframe, and coordinates mainframe discovery and polling. After *cwbhcid* is initiated, it starts the following daemons:

- **cwbhcmdd**—Sends commands to the mainframe.
- **cwbhmond**—Coordinates mainframe discovery and polling.

cwb start cwbhcid [-h | -v] *domain_name*

Syntax Description

-h	Displays a help message.
-v	Displays the version.
domain_name	Enter the name of the host domain.

Defaults

No default behavior or values.

cwbhcmdd

The Host Command Interface daemon (cwbhcmdd) runs in the workstation to send commands to the SNA mainframe. It is started by cwbhcid and should not be started by the user.

cwbhcmdd [-h | -v] *domain_name*

Syntax Description

-h	Displays a help message.
-v	Displays the version.
domain_name	Enter the name of the host domain.

Defaults

No default behavior or values.

cwbhmond

The Host Discovery/Poller daemon (cwbhmond) runs in the workstation to coordinate SNA mainframe discovery and polling. It is started by *cwbhcid* and should not be started by the user.

cwbhmond [-h | -v] *domain_name*

Syntax Description

-h	Displays a help message.
-v	Displays the version.
domain_name	Enter the name of the host domain.

Defaults

No default behavior or values.

CWB Command Script

This section describes the **cwb** command script that you run from */opt/CSCOcb/bin* to start the CiscoWorks Blue applications and includes the following subsections:

Starting and Stopping Servers

To start and stop the CiscoWorks Blue Process Manager and Name servers, use the **cwb** command.

cwb {start | stop} [**pm | name**]

cwb start servers

Syntax Description

start	Starts the specified process by the *process_name*.
stop	Stops the specified process by the *process_name*.
pm	Starts or stops the Process Manager server. The Process manager, starts all Maps and SNA View autostartable processes.
name	Starts or stops the CiscoWorks Blue (corba osagent) name server, which is required for using the Process Manager and Message Logger. When Process manager starts, it automatically starts the name server.
start servers	Starts all servers.

Defaults

No default behavior or values.

Usage Guidelines

You must be the root user to start and stop servers.

cwbdiscover

Cisco does not recommend that you start the discovery process from the command line because you will not see a progress indicator until discovery is complete. Instead, use the **cwb start admin** command to start the Administration application and run discovery from the Administration application.

If you want to use the command-line interface, then use the **cwb start cwbdiscover** command to start and stop the CiscoWorks Blue discovery processes. Each discovery process starts, discovers the devices, then stops.

To periodically run discovery processes to automatically discover new devices, run the **cwb start cwbdiscover** command as a UNIX *cron* job (chronologically started). Set the cron job to run at night or when system and network activity is low.

Use the discover processes to determine whether each IP device in your network is active and to verify which routers are enabled for each protocol. In addition to discovering the devices, the discovery process also sets the status and protocol fields in the Devices table.

If you have a dynamic network and expect to configure new or existing routers with DLSw, start the discovery process to ensure that the database used for your selected protocols reflects your current network topology.

After execution, the discover process queries all IP devices in the database that are flagged *not discovered*. A device is set to *not discovered* when one of the following occurs:

- The newly-added device has never been discovered for a specific protocol.
- A trap received from the device causes the Peer table to be updated.

If there is a NMS installed, the discover process can use the NMS database to synchronize the Maps database with the network management system's database. If not, the discover process requires a seed file to be used to add new devices to the database.

cwb start cwbdiscover [**-d** [**d**][**r**][**a**][**t**]]
[**-r** *read_community_string* [**-s** *seed_file_name*]]
[**-h**] [**-v**]

Syntax Description

-d [d][r][a][t]	Specifies one or more protocols to discover: • **d** discovers devices running the DLSw protocol. • **r** discovers devices running the RSRB protocol. • **a** discovers devices running the APPN protocol. • **t** discovers devices running the TN3270 protocol. If you specified the -d switch with no protocols, all protocols are discovered. If you enter multiple protocols, do not separate them with spaces.
-r *read_community_string*	Specifies a global read community string for all devices in the seed file that do not specify a read community string. If all read community strings are the same, enter the device name in the seed file and specify the read community string on the command line.
-s *seed_file_name*	Specifies a seed file. Replace *seed_file_name* with the seed file name.
-h	Displays a help message.
-v	Displays the version.

Defaults

No default behavior or values.

MIB Variables Queried During Discovery

This section lists the MIB variables queried during discovery. Maps and SNA View support the following MIBs:

- CISCO-RSRB-MIB
- CISCO-DLSW-MIB
- IBM-6611-APPN-MIB
- OLD-DLUR-MIB
- CISCO-TN3270-SERVER-MIB
- IETF draft standard DLSw MIB (RFC 2024)
- IETF draft standard APPN MIB (RFC 2455)
- IETF draft standard DLUR MIB (RFC 2232)

This section contains these main topics:

- Base Discovery MIB Variables
- RSRB Discovery MIB Variables
- DLSw Discovery MIB Variables
- APPN Discovery MIB Variables
- TN3270 Discovery MIB Variables

Note If you see SNMP failures when querying MIB variables during discovery, polling, or other user queries, which require SNMP responses (such as DLSw peer statistics), a malfunction may exist at the queried router. Please check with the manufacturer of the router being queried for MIB.

Base Discovery MIB Variables

The following variables are queried whenever discovery is run, no matter which protocol is being discovered:

sysObjectID	ipAdEntIfIndex
ifIndex	ipAdEntNetMask

ifType	dot1dSrPortLocalSegment
ifPhysAddress	dot1dSrPortBridgeNum
ipAdEntAddr	dot1dSrPortTargetSegment

RSRB Discovery MIB Variables

The RSRB discovery process queries the following CISCO-RSRB-MIB variables in addition to the base MIB variables. These variables are unique to RSRB:

rsrbRemotePeerEncapsulation	rsrbRemotePeerState
rsrbRingLocal	rsrbVirtRingIPAddr
rsrbRemotePeerIPAddr	rsrbRingBridge
rsrbRingType	

DLSw Discovery MIB Variables

The DLSw discovery process first queries the standard DLSW-MIB (RFC 2024). If that fails, the DLSw discovery process queries the CISCO-DLSW-MIB. The following DLSw MIB variables (unique to DLSw) are queried in addition to the base MIB variables:

DLSW-MIB (RFC 2024)	CISCO-DLSW-MIB
dlswNodeStatus	ciscoDlswStatus
dlswTConnOperLocalTAddr	ciscoDlswTConnOperLocalTAddr
dlswTConnOperConnectTime	ciscoDlswTConnOperConnectTime
dlswTConnOperState	ciscoDlswTConnOperState
dlswTConnOperConfigIndex	ciscoDlswTConnOperConfigIndex
dlswTConnConfigTDomain	ciscoDlswTConnConfigTDomain
dlswTConnConfigLocalTAddr	ciscoDlswTConnConfigLocalTAddr
dlswTConnConfigRemoteTAddr	ciscoDlswTConnConfigRemoteTAddr
dlswCircuitS1DlcType	ciscoDlswCircuitS1DlcType
dlswCircuitS1RouteInfo	ciscoDlswCircuitS1RouteInfo
dlswCircuitS2TDomain	ciscoDlswCircuitS2TDomain

DLSW-MIB (RFC 2024)	CISCO-DLSW-MIB
dlswCircuitS2TAddress	ciscoDlswCircuitS2TAddress
dlswCircuitState	ciscoDlswCircuitState

APPN Discovery MIB Variables

The following APPN MIB variables are queried during discovery:

APPN-MIB (RFC 2455)	IBM-6611-APPN-MIB
appnNodeCpName	ibmappnNodeCpName
appnNodeType	ibmappnNodeType
appnNodeBrNn	

TN3270 Discovery MIB Variables

The discovery process queries the device to determine whether it is configured with the *tn3270sCpuCard* TN3270 MIB variable.

Starting and Stopping Processes

To start and stop CiscoWorks Blue processes, use the **cwb** command.

cwb {start | stop} *process_name*

cwb stop all

Syntax Description

start	Requests the Process Manager to start a process using a *process_name*.
stop	Requests the Process Manager to stop one or more processes.
process_name	Specifies the process name of the process to stop or start.
stop all	Requests the Process Manager to: • Stop all running CiscoWorks Blue processes, including all clients and servers. • Stop the Process Manager and Name servers.

Defaults

No default behavior or values.

Starting and Stopping User Applications

This section describes how to start and stop user applications with the **cwb** command. This section contains the following information:

cwb start admin

To start the CiscoWorks Blue Administration application, use the **cwb start admin** command.

cwb start admin [**-p** *portno*] [**-v**] [**-h**]

Syntax Description

start	Starts the specified application.
admin	Starts the CiscoWorks Blue Administration application (cwbadmin), which lets you start and stop Maps and SNA View processes and discover network devices.
[**-p** *portno*]	Specifies a port number for discovery work-in-progress information. The first discovery process spawned uses the specified port number or the default port number. The default is 57193. For each subsequent spawned discover process, the port number is increment by 1. Subsequent discover processes are spawned when you select a protocol (say RSRB) first and start discover, then select another protocol (say DLSw) and start discover again. The second discover process uses a port number 1 greater than the first.
[**-v**]	Displays the version.
[**-h**]	Displays a usage statement.

Defaults

No default behavior or values.

cwb start dlsw

To start the CiscoWorks Blue Maps DLSw Motif application, use the **cwb start dlsw** command.

cwb start dlsw [**-u** *portno*] [**-p** *portno*] [**-k** | **-g**] [**-f** *device_name*] [**-v**] [**-h**]

Syntax Description

start	Starts the specified user application.
dlsw	Starts the DLSw GUI application, the DLSW executable, the DLSw poller daemon (**cwbdlswpollerd**), and the monitor daemon (**cwbmonitord**).
-u *portno*	Specifies a port for socket communications with the monitor daemon. The **runprocess** script defaults to port 6000. If the monitor daemon has been changed to listen to another port, make the same change in this option in the script.
-p *portno*	Specifies a port for socket communications with the discovery process when it is launched by the **dlsw** application. The **runprocess** script defaults to port 6011. If another application is using this port, you can specify another port with this option.
-k	Starts with the key devices view. This is the default.
-g	Starts with the global view.
-f *device_name*	Starts with the focus view for the specified device.
-v	Displays the version.
-h	Displays a usage help statement.

Defaults

No default behavior values.

cwb start rsrb

To start the CiscoWorks Blue Maps RSRB Motif application, use the **cwb start rsrb** command.

cwb start rsrb [**-u** *portno*] [**-p** *portno*] [**-g**] [**-f** *device_name*] [**-v**] [**-h**]

Syntax Description

start	Starts the specified user application.
rsrb	Starts the RSRB GUI application, the RSRB executable, the RSRB poller daemon (*cwbrsrbpollerd*), and the monitor daemon (*cwbmonitord*).
-u *portno*	Specifies a port for socket communications with the monitor process. The script defaults to port 6000. If the monitor daemon has been changed to listen to another port, make the same change in this option in the script.
-p *portno*	Specifies a port for socket communications with the discovery process when it is launched by the **rsrb** application. The script defaults to port 6001. If another application is using this port, you can specify another port with this option.
-g	Starts with the global view.
-f *device_name*	Starts with the focus view for the specified device.
-v	Displays the version.
-h	Displays a usage help statement.

Defaults

No default behavior or values.

cwb start appn

To start the CiscoWorks Blue Maps APPN Motif application, use the **cwb start appn** command.

cwb start appn [**-f** *device_name* [**-r** *read_community_string*]] [**-v**] [**-h**]

Syntax Description

start	Starts the specified user application.
appn	Starts the APPN GUI application, the APPN executable, and the APPN poller server daemon (*AppnPollerServer*).
-f *device_name*	Specifies the host name or IP address of an APPN node to be used as the network topology agent. This network topology agent also can be specified in the cwbinit file or omitted.
-r *read_community_string*	Specifies the read community string for the router specified by device_name. APPN uses the read_community_string when communicating with an APPN node. If you do not enter a read community string, the APPN application uses the default read community string specified in the cwbinit file or, if there is not one there, the default string "public."
-v	Displays the version.
-h	Displays a usage help statement.

Defaults

No default behavior or values.

MsgLogClient

To start the Message Log display client application, use the **cwb start MsgLogClient** command.

cwb start MsgLogClient

Syntax Description

start	Starts the specified user application.
MsgLogClient	Starts the Message Log client (viewer) application.

Defaults

No default behavior or values.

ProcMgrClient

To start the Process Manager display client application, use the **cwb start ProcMgrClient** command.

cwb start ProcMgrClient

Syntax Description

start	Starts the specified user application.
ProcMgrClient	Starts the Process Manager client (viewer) application.

Defaults

No default behavior or values.

cwb kill all Command

To terminate all running CiscoWorks Blue processes and servers, use the **cwb kill all** command.

cwb kill all

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Usage Guidelines

You must be the root user to use the **cwb kill all** command.

The **cwb kill all** command is intended for situations when processes or servers appear to be stuck in a transitional state (for example, starting or stopping) and do not appear to respond to the normal **cwb start** and **cwb stop** commands.

cwb show

To display information about the CiscoWorks Blue servers, use the **cwb show** command.

cwb show {versions | status}

Syntax Description

versions	Displays the version information about all CiscoWorks Blue servers.
status	Displays the current status and process IDs of all CiscoWorks Blue servers and processes. The last message column displays the last message sent by the processes to the Process Manager.

Defaults

No default behavior or values.

cwb tac

The **cwb tac** command runs the CiscoWorks Blue TAC collection program to collect and zip all the information you will need when you call the Cisco TAC. You must be the root user to use the **cwb tac** command.

cwb tac [-o *outputdirectory***]**

Syntax Description

-o *outputdirectory*	Specifies a directory where the command output is saved.
	
	If you omit this operand, the output is saved as file *cwbtac_n.tar.Z* in a temporary directory, where the *n is* incremented for each successive use. The **cwb tac** command searches for a temporary directory in this order: */usr/tmp*, */var/tmp*, */tmp*.
	
	You can specify an output directory in which to save the output of the **cwb tac** command:
	
	• You can specify an absolute directory by preceding the path with a / character. If the specified directory does not exist, the **cwb tac** command prompts you to create it. The following command saves the zipped file as */usr/cwblue/cwbtac_1.tar.Z*.
	
	`cwb tac -o /usr/cwblue`
	
	• You can specify a relative directory. This directory is always relative to */opt/CSCOcb/etc*. The following command saves the zipped file as */opt/CSCOcb/etc/tac/cwbtac_1.tar.Z*.
	
	`cwb tac -o tac`

Defaults

No default behavior or values.

cwb—Running Miscellaneous Applications

The **cwb** command runs the suite of miscellaneous CiscoWorks Blue applications.

cwb {create seed | clear db | check db | config | verify | tac}

Syntax Description

create seed [**-s** *seedfile*]	Creates a seed file from the devices in the CiscoWorks Blue database. **-s** *seedfile* specifies the name of the seed file to create. If you omit this parameter, the seed file is named *seed.file*.
clear db	Clears the CiscoWorks Blue Database and the *appnfile* file. All data will be lost. To regenerate, discovery must be run for all protocols. You must be the root user to use the **cwb clear db** command. The **cwb clear db** command stops all clients and servers, clears the database and the *appnfile* file, then restarts all servers.
check db	Checks the integrity of the database and offers alternatives if it is found to be suspect. The database can be synchronized with the log file and restored from a backup taken the last time the router discover process was performed or the **cwb maintenance** command was run. The database can be cleared completely to a point at which discovery must be rerun to restore the data. The **cwb check db** command runs automatically whenever the CiscoWorks Blue process manager is restarted with the **cwb start servers** command.

config	Runs the *cwbconfig* application to configure CiscoWorks Blue host connection and port usage. You must be the root user to use the **cwb config** command.
verify	Runs the CiscoWorks Blue verification program to verify that you installed the applications correctly, and to check your configuration files and the database.

Defaults

No default behavior or values.

Utilities and Commands

This section describes the following utilities and commands:

This section describes the following procedures:

uninstall.sh

Use the **uninstall.sh** command to uninstall CiscoWorks Blue Maps and SNA View applications. After you enter the **uninstall.sh** command, it detects all the installed Maps and SNA View files and asks you whether you want to delete them.

uninstall.sh

Syntax Description This command has no arguments or keywords.

Defaults No default behavior or values.

Usage Guidelines To uninstall the installed Maps applications, use the following command:

cd /opt/CSCOcb/install

./uninstall.sh

cgisnamaps Process

The *cgisnamaps* process is a cgi-bin program that is started when a CWBlue web page is launched. It passes data between the web browser and *cwbsnamapsd*. There are no operands and it should not be run by the user.

cwbsnamapsd

To get information from the database for distribution by the web server, run the cwbsnamapsd command in the workstation. You might want to stop and restart the web daemon for the following reasons:

- To obtain information about any newly-defined TN3270 PUs
- To use a different APPN network topology agent

cwb start cwbsnamapsd [**-h** | **-v**] [*interval*]

cwb stop cwbsnamapsd

Syntax Description

-h	Displays a help message.
-v	Displays the version.
interval	Specifies the number of seconds the daemon can wait from when it completes one cycle until it starts the next cycle.

Defaults

No default behavior or values.

Usage Guidelines

After you change the *doDNSSearch* parameter in the *cwbinit* file, you should stop and restart *cwbsnamapsd*.

runprocess

Use the **runprocess** command, in the *$CWBROOT/etc* directory to set appropriate environment variables and then execute a command.

runprocess *process_name*

Syntax Description

process_name	The name of the Maps process to be executed.

Defaults

No default behavior or values.

Usage Guidelines

You should not use **runprocess** directly, but you might want to edit the script to change selected arguments.

cwbupgrade.sh

To have the system prompt you to enter the Maps and SNA View license keys after installation, use the **cwbupgrade.sh** command.

cwbupgrade.sh

Syntax Description

This command has no arguments or keywords.

Defaults

No default behavior or values.

Changing Message Logging For Each Process

Most CiscoWorks Blue processes and executables, by default, store Error, Warning, and Info messages in the message log. The Error and Info messages are logged automatically. A parameter in the */opt/CSCOcb/etc/runprocess* script sets additional default values for the level of debugging messages that each process logs in the message log. At installation, each process is set to log Warning messages. If you must change these default values, you can edit the STD_DBG_PARAM statements in */opt/CSCOcb/etc/runprocess*.

Using Message Log Client to Control Message Logging

The normal mode of operation is to use the Message Log client to dynamically control message logging for each process. To control message logging during process startup, or if you want to make message log changes permanent, modify the *runprocess* script as described. Enabling additional message logging can hurt performance and cause web time outs. Enable additional message logging only when necessary or when requested by Cisco TAC.

Example CiscoWorks Blue Process

For each CiscoWorks Blue process, there is an entry in */opt/CSCOcb/etc/runprocess* that starts with a **case** statement. This example shows the entry for the DLSw poller daemon (cwbdlswpollerd):

```
case cwbdlswpollerd:
set STD_DBG_PARAM="-MLCenableFilters Warning"
set GIVEN_PARAM="${GIVEN_PARAM} ${STD_DBG_PARAM}"
set PARAMETERS="${PM_PARAM} ${ML_PARAM} ${ORB_PARAM} ${GIVEN_PARAM}"
eval exec $CWBROOT/dlsw/bin/cwbdlswpollerd $PARAMETERS
breaksw
```

Look at the highlighted line that contains the STD_DBG_PARAM statement. The -MLCenableFilters parameter, in this case, specifies that Warning messages are to be logged.

MLCenableFilters Syntax

The format of the MLCenableFilters parameter is shown below.

Parameter	MLCenableFilters token1[:token2 ... :token*n*]
token1[**:token2 ... :token***n*]	One or more message severity codes separated by colons(:). The allowable message severity codes are: **Debug**—Useful when debugging a problem in conjunction with Cisco's Technical Assistance Center. **Error**—Generates messages when any operational error condition occurs. **Warning**—Generates messages when an error condition, which is not fatal occurs. **Info**—Generates messages to notify you of status information. **Trace**—Generates detailed operational log messages. **SNMPTrace**—Generates detailed SNMP trace log messages. **UITrace**—Generates trace log messages from user interface. **IPCTrace**—Generates detailed log messages for socket operations and interprocess communication. **Dump**—Generates dumps. **InternalTrace**—Generates internal operational log messages. The Error and Info message categories are enabled automatically.

For example, to enable the logging of Warning, Debug, and Dump messages, in addition to the default Error and Info messages, for the DLSw poller daemon, you might edit */opt/CSCOcb/etc/runprocess* and change the **case** statement for cwbdlswpollerd to look like this:

```
case cwbdlswpollerd:
set STD_DBG_PARAM="-MLCenableFilters Warning:Debug:Dump"
set GIVEN_PARAM="${GIVEN_PARAM} ${STD_DBG_PARAM}"
set PARAMETERS="${PM_PARAM} ${ML_PARAM} ${ORB_PARAM} ${GIVEN_PARAM}"
eval exec $CWBROOT/dlsw/bin/cwbdlswpollerd $PARAMETERS
breaksw
```

Exceptions

The following CiscoWorks Blue processes do not support the MLCenableFilters parameter:

- CreateSeedFile
- The HP versions of the **appn**, **dlsw**, and **rsrb** executables and *PollerServer.*

Changing Parameters on Process Calls

If you just want to make the process calls use the **-h** (help) and **-v** (version) arguments, issue one of these commands directly, instead of editing the script:

```
/opt/CSCOcb/etc/runprocess pnam -h
/opt/CSCOcb/etc/runprocess pnam -v
```

All the CiscoWorks Blue applications are started with the **runprocess** script. If you want to change the parameters with which an application is started, you can edit the **runprocess** script to change the arguments.

Step 1 First see if the arguments you want to change are in the *cwbinit* file. If so, change them there instead.

Step 2 Before you change **runprocess**, make a backup copy.

Step 3 Edit the */opt/CSCOcb/etc/runprocess* file.

Step 4 Search for the line that begins with the word **case** and contains the name of the application you want to change. For example, the line for the RSRB poller is as follows:

```
case cwbrsrbpollerd:
```

Step 5 Look after the case line for the line that starts with *set PARAMETERS*. For the DLSw poller, that line looks like the following:

```
set PARAMETERS="${PM_PARAM} ${ML_PARAM} ${ORB_PARAM} ${GIVEN_PARAM}"
```

Step 6 Insert the arguments at the end of the *set PARAMETERS* line, just before the closing double quotes, and after leaving a space. For example, to change the polling sleep time for the RSRB poller to 600 seconds, you would add the value 600 to the *set PARAMETERS* line as follows:

```
set PARAMETERS="${PM_PARAM} ${ML_PARAM} ${ORB_PARAM} ${GIVEN_PARAM}
600"
```

Step 7 Save the file.

CiscoWorks Blue Maps and SNA View Web Interface

This appendix provides information about how to access various functions of the CiscoWorks Blue Maps and SNA View applications by supplying a URL containing function calls and parameters. Use the information in this appendix to program links from other web pages directly to any CiscoWorks Blue Maps or SNA View web page. Your end users will find navigation through the product easier if they start at the CiscoWorks Blue home page.

The general form of the URL is as follows:

http://*nnnnnnn:pppp***/cgi-bin/cw-blue/snamaps?rqx=***#&p1&p2&p3…..&pn***

Where:

nnnnnnn represents the IP Address or the IP Host Name of the Maps and SNA View web server

pppp represents the IP Port number associated with the Maps and SNA View web server (optional - defaults to port 80. This value is assigned during Maps and SNA View installation)

represents the request type (1-11). The request types are described in the following section.

&p1&p2…&pn represents the filter parameters for the various request types. The parameters are described in the following section.

Using Web Interface Functions

rqx=1

CiscoWorks Blue Maps APPN/SNASw Network Management

This function presents the APPN/SNASw Network Management panel.

Parameters

There are no required parameters for this function.

Example

http://shada/cgi-bin/cw-blue/snamaps?rqx=1

rqx=2

CiscoWorks Blue Maps DLSw Network Management

This function presents the DLSw Network Management panel.

Parameters

There are no required parameters for this function.

Example

http://shada/cgi-bin/cw-blue/snamaps?rqx=2

rqx=3

CiscoWorks Blue Maps RSRB Network Management

This function presents the RSRB Network Management panel.

Parameters

There are no required parameters for this function.

Example

http://shada/cgi-bin/cw-blue/snamaps?rqx=3

rqx=4

CiscoWorks Blue SNA Resource Information

This function presents the Basic or Advanced Search Panel for SNA Resource Information. The presentation of the Basic or Advanced Search Panel is determined by the user's preference set in the Options Panel.

Parameters

There are no required parameters for this function.

Example

http://shada/cgi-bin/cw-blue/snamaps?rqx=4

rqx=5

CiscoWorks Blue Utilities Menu

This function presents the CiscoWorks Blue Utilities Menu, which allows you to run the verification utility, log on to NetView, or reset to the default parameters.

Parameters

There are no required parameters for this function.

Example

http://shada/cgi-bin/cw-blue/snamaps?rqx=5

rqx=6

CiscoWorks Blue Options Menu

Use this function to set preferences for the display of MAC addresses and RIF fields, and set up the hotlinks for NetView and CiscoWorks 2000.

Parameters

There are no required parameters for this function.

Example

http://shada/cgi-bin/cw-blue/snamaps?rqx=6

rqx=7

CiscoWorks Blue SNA View Basic Search

This function is called from a completed Basic Filter panel. It is used to search the CiscoWorks Blue SNA View database and provide a Filter Results Panel. If the supplied parameters uniquely identify a session, the Session Connectivity Display for the session is displayed.

Parameters

The possible parameters are described as follows:

Paramter	Description
&bn=	Fully qualified or wild-carded resource name (&bn, &bt, or &bm must be provided) Format is xxxxxxxx.yyyyyyyy Where: xxxxxxxx is the resource name .yyyyyyyy is the domain name (optional)
&bnt=	Resource Type l&bn—Logical Unit name p&bn—Physical Unit name (default) c&bn—Control Point name i&bn—XID
&bt=	TN3270 Client Host Name or IP Address (&bn, &bt, or &bm must be provided)
&bp=	TN3270 Client Port Address (requires that &bt be provided)
&bm=	MAC Address (&bn, &bt, or &bm must be provided)
&bs=	SAP Address (requires that &bm be provided)

Paramter	Description
&bmx=	Maximum number of sessions (The default is 100.)
&bem=on	Exact Matches only (delete parameter to get generic matches)

Note See the CiscoWorks Blue Maps and SNA View User Guide for additional information on data formats.

Example

To get the view for a physical unit named EBC4, use the following:

http://shada/cgi-bin/cw-blue/snamaps?rqx=7&bn=EBC4

rqx=8

CiscoWorks Blue SNA View Advanced Search

This function is called from a completed Advanced Filter panel. It is used to search the CiscoWorks Blue SNA View database and provide a Filter Results Panel. If the supplied parameters uniquely identify a session, the Session Connectivity Display for the session is displayed. This function differs from the Basic Search by allowing combinations of LU, PU, CP, and XID names.

Parameters

The possible parameters are described as follows:

Parameter	Description
&pu=	Fully qualified or wild-carded Physical Unit name (&pu, &lu, &cp, or &xi must be provided) Format is xxxxxxxx.yyyyyyyy Where: xxxxxxxx is the resource name .yyyyyyyy is the domain name (optional)
&lu=	Fully qualified or wild-carded Logical Unit name (&pu, &lu, &cp, or &xi must be provided) Format is xxxxxxxx.yyyyyyyy Where: xxxxxxxx is the resource name .yyyyyyyy is the domain name (optional)
&cp=	Fully qualified or wild-carded Control Point name (&pu, &lu, &cp, or &xi must be provided) Format is xxxxxxxx.yyyyyyyy Where: xxxxxxxx is the resource name .yyyyyyyy is the domain name (optional)
&xi=	Fully qualified IDBLK/IDNUM (&pu, &lu, &cp, or &xi must be provided) Format is exactly 10 hexadecimal digits beginning with 0x 0x12345678, 0x123/45678, 0x123-45678, 0x123,45678
&tc=	TN3270 Client Host Name or IP Address
&po=	TN3270 Client Port Address (requires that &bt be provided)

Parameter	Description
&ma=	MAC Address Format: 0x123456789ab
&sa=	SAP Address (requires that &bm be provided) Format 0x04
&de=	Dependent Router Name
&dr=	DLUR name Format is xxxxxxxx.yyyyyyyy Where: xxxxxxxx is the resource name .yyyyyyyy is the domain name (optional)
&ds=	DLUS name Format is xxxxxxxx.yyyyyyyy Where: xxxxxxxx is the resource name .yyyyyyyy is the domain name (optional)
&mx=	Maximum number of sessions (The default is 100)
&em=on	Exact Matches only (delete parameter to get generic matches)
&pr=	Protocol Possible values are d(=dlsw), r(=rsrb), a(=appn), t(=tn3270), o(=other)
&p4=	PU4/Node name.

Note See the CiscoWorks Blue Maps and SNA View User Guide for additional information on data formats.

Example

To get the view for a logical unit named EBC4, use the following:

http://shada/cgi-bin/cw-blue/snamaps?rqx=7&bn=EBC4

rqx=9

CiscoWorks Blue Maps APPN/SNASw Views

This function is called from the APPN/SNASw Network Management Screen, and determines whether a Network Topology View or a Node Details View is provided. This function can be used to provide a Node Details View for a router.

Parameters

The possible parameters are described as follows:

Parameter	Description
&a=	Determines the type of view (required nt—APPN Network Topology View nd—APPN Node Detail View
&ip=	IP address or Host Name of Network Node for Network Topology View or Node Detail View (requires &rc= parameter) Either &ip= or &cp= parameter must be specified
&rc=	Read Community String
&cp=	APPN Control Point name for Network Topology View or Node Detail View Either &ip= or &cp= parameter must be specified

Example

To get the Node Detail View for a router named bonzo, use the following:

http://shada/cgi-bin/cw-blue/snamaps?rqx=9&a=nd&ip=bonzo&rc=public

rqx=10

CiscoWorks Blue Maps DLSw Views

This function is called from the DLSw Network Management Screen, and determines whether a DLSw Global View, a DLSw Key Devices View, or a DLSw Focus View is provided. This function can be used to provide a Focus View for a router.

Parameters

The possible parameters are described as follows:

Parameter	Description
&a=	Determines the type of view (required) g—DLSw Global View k—DLSw Key Devices View f—DLSw Focus View (requires &f= parameter)
&f=	Focus Router Name

Example

To get the Focus View for a router named berima, use the following:

http://shada/cgi-bin/cw-blue/snamaps?rqx=10&a=f&f=berima

rqx=11

CiscoWorks Blue Maps RSRB Views

This function is called from the RSRB Network Management Screen, and determines whether an RSRB Global View, an RSRB Focus View, or an RSRB Virtual Ring View is provided. This function can be used to provide a Focus View for a router.

Parameters

The possible parameters are described as follows:

Parameter	Description
&a=	Determines the type of view (required) g—RSRB Global View v—RSRB Virtual Ring View Requires &r= parameter f—RSRB Focus View (requires &f= parameter)
&f=	Focus Router Name
&r=	Virtual Ring Number

Example

To get the Focus View for a router named berima, enter the following:

http://shada/cgi-bin/cw-blue/snamaps?rqx=11&a=f&f=berima

Mainframe and Workstation Installation Checklist

This appendix provides a list of the parameters that must be coordinated between the mainframe configuration and the workstation configuration. Cisco recommends that mainframe or workstation installers agree on these values before the mainframe or workstation installation is started.

This appendix provides information about the following two types of parameters:

TCP/IP Connection Parameters

The following table lists the TCP/IP parameters that configure TCP/IP connection between the mainframe and the workstation. These parameters are contained in the */etc/svopen_config_DOMAINNAME* file that you configure using a text editor. The related mainframe parameters are set using the TCP parameter card in the NSPPARM member. The following worksheet lists the TCP/IP configuration parameters.

TCP/IP Configuration Parameters Worksheet

TCP/IP host name or address of the mainframe:		
Mainframe value:		_____
Workstation value:	SVMF_AGENT_ADDR=	_____
Default:		None
Connection protocol:		
Mainframe value:		TCP parameter card
Workstation value:	SVMF_CONNECT=	TCP
Default:		None
Host connection interface port:		
Mainframe value:		_____
Workstation value:	SVMF_HCI_AGENT_PORT=	TCP *HCS_port* _____
Default:		6104
Host command server port:		
Mainframe value:		
Workstation value:	SVMF_CMDS_AGENT_PORT=	TCP _____ *HCS_port*
Default:		6105

The TCP/IP address of the mainframe is the host name or IP address of the mainframe on which the mainframe application is installed. Use the SVMF_AGENT_ADDR parameter in the workstation */etc/vopen_config_DOMAINNAME* file.

The connection protocol is the communication protocol between the mainframe and the workstation. The SVMF_CONNECT parameter indicates whether the workstation will connect to the mainframe using TCP/IP. To connect via TCP/IP,

specify **SVMF_CONNECT = TCP** in the workstation */etc/svopen_config_DOMAINNAME* file and provide a TCP parameter card at the mainframe.

The host connection interface port is the port number used by the host connection interface. Use this port number in the SVMF_HCI_AGENT_PORT parameter in the workstation */etc/svopen_config_DOMAINNAME* file and on the mainframe TCP parameter card.

The host command server port is the port number used by the host command server. Use this port number in the SVMF_CMD_AGENT_PORT parameter in the workstation */etc/svopen_config_DOMAINNAME* file and on the mainframe TCP parameter card.

Coding the TCP Parameter Card

Use the TCP parameter card at the mainframe to identify the ports to be used for the host command server and the host connection interface. The TCP parameter card has the following format:

```
TCP hciport cmdport
```

Where:

hciport is the port for the host connection interface (usually 6104).

cmdport is the port for the host command server (usually 6105).

LU 6.2 Parameters

This section describes an additional set of parameters for connecting UNIX workstations to the mainframe using LU 6.2. The following worksheet lists the LU 6.2 parameters.

Note Before you configure LU 6.2, the mainframe and workstation must be already configured to support an LU 6.2 connection between them. The mainframe application configuration adds only the information necessary for the workstation application to communicate with the mainframe application. Items like the Remote Link address have been omitted, since this should be already configured.

LU 6.2 Configuration Parameters Worksheet

Connection protocol:	
Mainframe value:	LU62 parameter card
Workstation value: SVMF_CONNECT=	LU62
Default:	None
Secondary independent LU:	
Mainframe value:	_____
Workstation value:	_____
Default:	None
Log mode:	
Mainframe value:	PARALLEL
Workstation value:	PARALLEL
Default:	PARALLEL
Message transaction program:	
Mainframe value:	NSPOPNMS
Workstation value:	NSPOPNMS
Default:	NSPOPNMS

Command transaction program:	
Mainframe value:	NSPOPNCS
Workstation value:	NSPOPNCS
Default:	NSPOPNCS

The connection protocol is the communication protocol between the mainframe and the workstation. The SVMF_CONNECT parameter indicates whether the workstation will connect to the mainframe using LU 6.2. To connect via TCP/IP, specify **SVMF_CONNECT=LU62** in the */etc/svopen_config_DOMAINNAME* file and provide a TCP parameter card at the mainframe.

The logmode specifies the VTAM logmode entry. Use PARALLEL on the SERVER parameter card.

The message transaction program identifies the workstation message server transaction program (MESSAGE_TP). Code NSPOPNMS on the SERVER parameter card.

The command transaction program identifies the workstation command server transaction program (COMMAND_TP). Code NSPOPNCS on the SERVER parameter card.

Coding the SERVER Parameter Card

You specify the mainframe parameters on the SERVER card in the NSPPARM member in the mainframe samples data set:

```
SERVER plu slu PARALLEL NSPOPNMS NSPOPNCS
```

Where:

plu is the label of the VTAM APPL definition that you coded with APPC=YES, that is the primary LU for the mainframe.

slu is the label of a CDRSC for the independent secondary LU defined for the workstation and associated with the workstation application PU.

PARALLEL is the logmode.

NSPOPNMS is the name of the SNA LU 6.2 transaction program for the workstation message server (MESSAGE_TP). You must use NSPOPNMS.

NSPOPNCS is the name of the SNA LU 6.2 transaction program for the workstation command server (COMMAND_TP). You must use NSPOPNCS.

Defining the Workstation SNA Package

On the workstation, configure LU 6.2 workstation parameters using the SNA package (Communications Server for AIX or SNAplusLink). Use the following values:

- The independent secondary LU defined for the workstation must match the *slu* parameter on the mainframe SERVER card.
- The workstation message server (MESSAGE_TP) is NSPOPNMS.
- The workstation command server (COMMAND_TP) is NSPOPNCS.
- The log mode is PARALLEL.

Symbols

Numerics

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

R

S

T

U

V

W

X

General Information

1 Years of networking experience _____ Years of experience with Cisco products _____

2 I have these network types: ☐ LAN ☐ Backbone ☐ WAN
☐ Other: _____

3 I have these Cisco products: ☐ Switches ☐ Routers
☐ Other: Specify model(s) _____

4 I perform these types of tasks: ☐ H/W Install and/or Maintenance ☐ S/W Config
☐ Network Management ☐ Other: _____

5 I use these types of documentation: ☐ H/W Install ☐ H/W Config ☐ S/W Config
☐ Command Reference ☐ Quick Reference ☐ Release Notes ☐ Online Help
☐ Other: _____

6 I access this information through: ____% Cisco Connection Online (CCO) ____% CD-ROM
____% Printed docs ____% Other: _____

7 Which method do you prefer? _____

8 I use the following three product features the most:

Document Information

Document Title: CiscoWorks Blue Maps and SNAView Workstation Installation and Administration Guide

Part Number: 78-11350-02 S/W Release (if applicable): Release 3.0.1

On a scale of 1–5 (5 being the best) please let us know how we rate in the following areas:

_____ The document was written at my technical level of understanding.
_____ The document was complete.
_____ The information was well organized.
_____ The information was accurate.
_____ The information I wanted was easy to find.
_____ The information I found was useful to my job.

Please comment on our lowest score(s):

Mailing Information

Company Name Date

Contact Name Job Title

Mailing Address

City	State/Province	ZIP/Postal Code
Country	Phone ( )	Extension
Fax ( )	E-mail	

Can we contact you further concerning our documentation? ☐ Yes ☐ No

You can also send us your comments by e-mail to **bug-doc@cisco.com**, or fax your comments to us at **(408) 527-8089**.