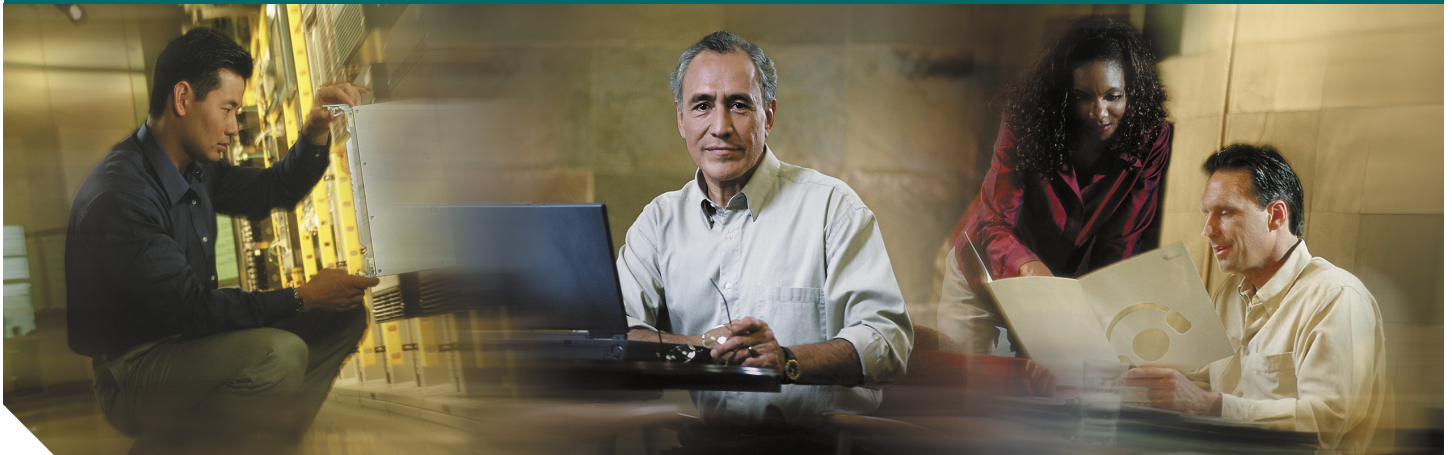




Cisco Craft Works Interface Quick Start Guide

Cisco IOS XR Software Release 3.2

- 1** Introduction
- 2** About the CWI
- 3** Getting Started
- 4** Setting Up the Router and CWI Client
- 5** Getting Started with the CWI
- 6** Locking and Unlocking the CWI
- 7** Installing and Accessing Online Help
- 8** Closing the CWI
- 9** CWI Supported Connection Methods and Applications
- 10** CWI Desktop Window
- 11** Configuration Desktop Window
- 12** Obtaining Documentation
- 13** Documentation Feedback
- 14** Cisco Product Security Overview
- 15** Obtaining Technical Assistance
- 16** Obtaining Additional Publications and Information



1 Introduction

This document introduces the Craft Works Interface (CWI) that supports Cisco IOS XR Software Release 3.2. The following sections are provided:

- About the CWI, page 2
- Getting Started, page 3
- Setting Up the Router and CWI Client, page 7
- Getting Started with the CWI, page 11
- Locking and Unlocking the CWI, page 19
- Installing and Accessing Online Help, page 19
- Closing the CWI, page 20
- CWI Supported Connection Methods and Applications, page 20
- CWI Desktop Window, page 21
- Configuration Desktop Window, page 23
- Obtaining Documentation, page 26
- Documentation Feedback, page 26
- Cisco Product Security Overview, page 27
- Obtaining Technical Assistance, page 28
- Obtaining Additional Publications and Information, page 29

Related Documentation

See the following list for related documents that may be useful:

- *Cisco Craft Works Interface User Interface Guide*
- *Cisco Craft Works Interface Configuration Applications Reference Guide*
- *Cisco Craft Works Interface Configuration Guide*

Intended Audience

This document is intended for experienced service provider administrators, Cisco telecommunication management engineers, and third-party field service technicians who have completed the required Cisco router training sessions.

2 About the CWI

The CWI is a client-side application used to configure and manage routers. The management and configuration features include fault management, configuration, security, and inventory, with an emphasis on speed and efficiency.

The CWI provides a context-sensitive graphical representation of the objects in a router, simplifying the process of configuring and managing the router. The CWI allows you to log in to multiple routers and perform the following management tasks:

- View, filter, sort, search, correlate, purge, and monitor real-time alarms.
- View, filter, export, and search real-time inventory and interface object attribute information.
- View and modify a configuration.
- Display a dynamic graphical representations of routers.
- Telnet/Secure Shell (SSH) to the router for command-line interaction. Troubleshoot management connectivity problems.

CWI provides the following features:

- A user-friendly context-sensitive interface that is used for fault, configuration, inventory, and security management of a router.
- A combination of both graphical and text-based interfaces that allow the user to select the best interface for the task at hand.
- A powerful CWI feature set used to simplify managing the router scale and complexity.
- Access to the powerful manageability features of the router.

The following features are common among the CWI applications:

- Printing, exporting, and searching data.
- Sorting and moving columns.
- Filtering records.
- Setting preferences.

See the *Cisco Craft Works Interface User Interface Guide* for details on common elements and procedures for common activities in the CWI Desktop.

CWI provides multiple methods to connect to the router:

- Serial Port
- Terminal Server
- CLI over Telnet/SSH
- XML over Telnet/SSH
- XML over CORBA

The CWI provides three ways to configure a router:

- Using the Terminal, Telnet or SSH applications launched from the CWI, which allows you to configure and manage the router using command-line interface (CLI) commands.
- Using the Configuration Editor or Replace Configuration Editor, which allows you to view and edit the running configuration in CLI format. The configuration editors provide common text editing functionality as well as traditional CLI features. See the “Replace Configuration Editor” section on page 25.
- Using the graphical configuration applications. See the “Configuration Desktop Window” section on page 23.

Controls are provided to manage the two-stage configuration process, which includes locking and rollback control.

3 Getting Started

This section provides information you need to know before you can start setting up a router and CWI client. Note that the specific setup is dependent on the session used from the About The CWI section. The following information is provided:

- Network Considerations, page 3
- Prerequisites, page 5

Network Considerations

The following network information must be taken into consideration before starting the minimum router and CWI client configuration.

Network Security

The default configuration is not secure. See the “Setting Up the Required Management Services Without a Secure Connection” section on page 8 for procedures.

Secure Socket Layer Encryption Configuration

The secure configuration uses Secure Socket Layer (SSL) encryption. If you use the SSL protocol on your network, use the SSL configuration. See the “Setting Up the Required Management Services with a Secure Connection” section on page 8 for procedures.

IP Security

IP security (IPSec) does not require any special configuration for CWI on the router or client. See the “Setting Up the Required Management Services Without a Secure Connection” section on page 8 for procedures.

Firewall

If you have a firewall in your network, you can use the basic or SSL encryption configurations. See the “Setting Up the Required Management Services with a Secure Connection” section on page 8 and “Setting Up the Required Management Services Without a Secure Connection” section on page 8 for procedures.

You must open the ports listed in Table 1 when configuring the firewall. See the firewall documentation for information on opening the ports.

Table 1 **Firewall Ports**

Component	Port	Direction
HTTP/HTTPS	80/443	Inbound
CORBA/CORBA SSL	10001/10002	Inbound
CORBA Notifications	49901 to 49950	Outbound
Telnet/SSH	23/22	Inbound/Outbound

Virtual Private Network

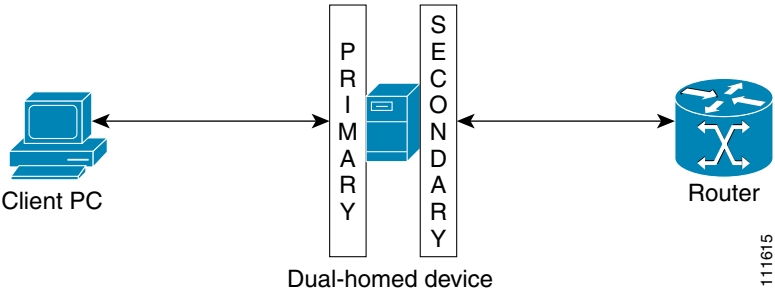
When setting the minimum router configuration you must use the client Virtual Private Network (VPN) IP address and Domain Name Server (DNS) name instead of the client IP address and DNS name when configuring the IP hostname for the CWI client. This mapping is required for the client to receive notifications from the router. See the “Router Prerequisites” section on page 7.

If you have a VPN, you can use the basic or SSL encryption configurations. See the “Setting Up the Required Management Services with a Secure Connection” section on page 8 and “Setting Up the Required Management Services Without a Secure Connection” section on page 8 for procedures.

Dual-Homed

Dual-homed devices are used to bridge two networks. You can run an instance of CWI on the dual-homed device so that you can access the secondary network. You will require terminal services or X-client software to run the CWI graphical application from the client PC. A dual-homed device contains a client-side interface (IP address) and router-side interface (IP address). The client-side is the primary interface, and the router-side is the secondary interface (see Figure 1).

Figure 1 *Dual-Homed Device Configuration*



When setting the minimum router configuration you must use the dual-homed device router-side (secondary) IP address and DNS name when configuring the IP hostname for the CWI client. This mapping is required for the client to view the notifications from the router received by the dual-home instance of CWI. See the “Router Prerequisites” section on page 7.

If you have a dual-homed device in your network, you can use the standard or SSL encryption configurations. See the “Setting Up the Required Management Services with a Secure Connection” section on page 8 and “Setting Up the Required Management Services Without a Secure Connection” section on page 8 for procedures.

Prerequisites

Prerequisites ensure that the CWI client and router are correctly set up to allow them to communicate. Meeting all prerequisites before starting any of the procedures in this guide is recommended to ensure successful communication between the CWI client and router.

The following prerequisites are provided:

- CWI Client System Prerequisites, page 5
- Router Prerequisites, page 7
- CWI Client Prerequisites, page 7



Note If you are using the CORBA connections and require notifications, the router must be explicitly configured for each client that is to receive notifications. These notifications include real-time inventory updates (for example online insertion and removal [OIR]), alarms, and change of configuration events. See the “Router Prerequisites” section on page 7 for information on configuring the router to send notifications to a specified client.

CWI Client System Prerequisites

The CWI client hardware requirements ensure that the CWI client has the proper verified system requirements for the chosen platform.

The following system requirements for a CWI client are provided in the hardware platform tables:

- Windows-based PC (see Table 2)
- UNIX (see Table 3)
- Linux (see Table 4)
- Macintosh (see Table 5)

Table 2 *Windows-Based PC Minimum System Requirements*

Requirement Type	Minimum Requirements
System hardware	IBM PC-compatible 500 MHz PentiumIII minimum, 1.20 GHz Pentium IV recommended.
System software	Windows 2000 or Windows XP.
Memory (RAM)	256 MB minimum, 512 MB recommended.

Table 2 Windows-Based PC Minimum System Requirements (continued)

Requirement Type	Minimum Requirements
Available drive space	CWI=5MB, JRE=48MB.
Additional software	One of these browsers: • Microsoft Internet Explorer 5.0 or higher. • Netscape Navigator 7.0 or higher. Java Runtime environment (JRE) version 1.4.2.
Monitor display settings	Minimum recommended screen resolution=1024 by 768 pixels.

Table 3 UNIX Minimum System Requirements

Requirement Type	Minimum Requirements
System hardware	Solaris 550 MHz minimum, 1.2GHz recommended.
Operating System	Solaris 7, 8, 9 (each with a full set of required Solaris patches).
Memory (RAM)	256 MB minimum, 512 MB recommended.
Available drive space	CWI=5MB, JRE=48MB.
Additional software	Netscape Navigator 7.0 or higher. JRE version 1.4.2. See the Sun website for latest minimum system requirements for the JRE on Solaris.
Monitor display settings	Minimum recommended screen resolution=1024 by 768 pixels.

Table 4 Linux-Based PC Minimum System Requirements

Requirement Type	Minimum Requirements
System hardware	IBM PC-compatible 500 MHz PentiumIII minimum, 1.20 GHz Pentium IV recommended.
Operating System	Red Hat Linux release 7.1 (Seawolf) or any Linux operating system on which Java Development Kit (JDK) 1.4.2 runs.
Memory (RAM)	256 MB minimum, 512 MB recommended.
Available drive space	CWI=5MB, JRE=48MB.
Additional software	Netscape Navigator. JRE version 1.4.2. See the Sun website for latest minimum system requirements for the JRE on Linux.
Monitor display settings	Minimum recommended screen resolution=1024 by 768 pixels.

Table 5 Macintosh Minimum System Requirements

Requirement Type	Minimum Requirements
System hardware	500 MHz minimum, 1.20 GHz recommended.
Operating System	MAC OS X 10.
Memory (RAM)	256 MB minimum, 512 MB recommended.
Available drive space	CWI=5MB, JRE=48MB.

Table 5 **Macintosh Minimum System Requirements (continued)**

Requirement Type	Minimum Requirements
Additional software	Safari version 1.2.3. JRE version 1.4.2.
Monitor display settings	Minimum recommended screen resolution=1024 by 768 pixels.

Router Prerequisites

The router prerequisites ensure that the router is correctly set up.

You must meet the following router prerequisites before logging in to a router using the CWI:

- Ensure that the Base image and Manageability pie have been installed and running on the router that you will be connecting to using the CWI client. Optionally, install and activate the Cisco IOS XR Security Package (K9SEC) to enable SSH and SSL functionality, and the MPLS pie to enable a Multiprotocol Label Switching (MPLS) configuration. See the *Cisco IOS XR Getting Started Guide* for information on how to start the base image.
- The minimum router configuration must be set before configuring the CWI client and required Management Services.
- For TTY or CORBA connection methods, ensure that connectivity is established between the router Management Ethernet interface and the CWI client. See the *Cisco IOS XR Getting Started Guide* for information on connecting an Ethernet interface from the CWI client to the router.
- At least one username and password must be configured on the router. A valid authentication, authorization, and accounting (AAA) username and password for accessing the router must be configured. See the *Cisco IOS XR Getting Started Guide* for information on configuring usernames and passwords on the router.

CWI Client Prerequisites

Ensure that the CWI client is correctly set up to communicate with the router. You should test the client connection. No special configuration is required on the CWI client.

Contact your system administrator to obtain the following information required to configure the router for use with the CWI:

- Router hostname.
- CWI client IP address if the client DNS name is not registered in a DNS server accessible by the router.

4 Setting Up the Router and CWI Client

This section provides the procedures that must be completed, in sequence, before you can start using the CWI. The procedures include setting the minimum router configuration that will allow the router to communicate with the CWI client, configuring the required Management Services, and configuring the CWI client.

See the *Cisco IOS XR Getting Started Guide* for information on the capabilities of the router, installing Cisco IOS XR software packages on the router, and booting up the router.

Setting Up Secure and Nonsecure Client Connections

When setting up the required Management Services, you have the option of communicating between the CWI client and required Management Services using SSL (secure connection) or no SSL (nonsecure connection).

The following two sections provide procedures for setting up the required Management Services with or without a secure connection:

- Setting Up the Required Management Services Without a Secure Connection, page 8
- Setting Up the Required Management Services with a Secure Connection, page 8

The “Testing the CWI Client” section on page 10 provides information on setting up the CWI client after the required Management Services are set up. The “Troubleshooting Basic IP Connectivity” section on page 11 provides information on resolving connectivity problems.

Setting Up the Required Management Services Without a Secure Connection

This section provides the procedures required to set up the required Management Services without SSL.

 **Note** The Telnet server must be enabled before you can manage a router using certain CWI features. These features include the Telnet application, setting character displays in the Rack View application, and viewing committed configuration changes using the Configuration Change dialog box. See the *Cisco IOS XR Getting Started Guide* for information on enabling the Telnet server.

 **Note** If you are connecting through a firewall in your network, the ports listed in Table 1 must be open before setting up the required Management Services. See your firewall documentation for information on opening the ports. See the “Network Considerations” section on page 3 for information on firewalls in a network.

To start the required Management Services on the router, perform the following steps:

Step 1 Establish a Telnet/SSH session with the router.

Step 2 Enter configuration mode.

```
RP/0/RP0/CPU0:router# configure
```

Step 3 Enable the HTTP server on the router.

```
RP/0/RP0/CPU0:router(config)# http server
```



Note If you are using either serial or terminal server connection modes, go to step6.

Step 4 Enable the Telnet server to log into the router using the IPv4 Telnet client.

```
RP/0/RP0/CPU0:router(config)# telnet ipv4 server max-servers [ <1-200> | no-limit ]
```

Step 5 Enable the XML agent on the router.

For CORBA XML agent:

```
RP/0/RP0/CPU0:router(config)# xml agent corba
```

For TTY XML agent:

```
RP/0/RP0/CPU0:router(config)# xml agent tty
```

Step 6 Exit configuration mode.

```
RP/0/RP0/CPU0:router(config)# commit
```

Setting Up the Required Management Services with a Secure Connection

This section provides the procedures required to set up the Management Services with SSL encryption. When setting up the required Management Services and the CWI client with a secure connection, the certification authority (CA) and router certificates must be set up before enabling the HTTP server and XML agent.

The following procedures are provided:

- Setting Up the Certificates, page 9
- Enabling the Secure HTTP Server and XML Agent, page 10

 **Note** The SSH server must be enabled before you can manage a router using certain CWI features. These features include the SSH application, setting character displays in the Rack View application, and viewing committed configuration changes using the Configuration Change dialog box. See the *Cisco IOS XR System Security Configuration Guide* for information on enabling the SSH server.

 **Note** If you are connecting through a firewall in your network, the ports listed in Table 1 must be open before setting up the required Management Services. See your firewall documentation for information on opening the ports. See the “Network Considerations” section on page 3 for information on firewalls in a network.

 **Note** You must have the Cisco IOS XR Security Package installed before attempting to complete the steps in this section. See the “Router Prerequisites” section on page 7.

 **Note** CWI does not support receiving notifications in CORBA SSL mode.

Setting Up the Certificates

 **Note** The CA and router certificates have to be set up only once on a router. If the certificates have been set up, proceed to the “Enabling the Secure HTTP Server and XML Agent” section on page 10.

To set up the certificates, perform the following steps:

Step 1 Establish a Telnet/SSH session with the router.

Step 2 Generate a Rivest, Shamir, and Adelman (RSA) key pair. Accept all prompted defaults.

```
RP/0/RP0/CPU0:router# crypto key generate rsa keypair-label
```

 **Note** If the key pair label is not specified, “the_default” will be used.

The following example is shown:

```
RP/0/RP0/CPU0:router# crypto key generate rsa key1
```

Step 3 Enter configuration mode.

```
RP/0/RP0/CPU0:router# configure
```

Step 4 Configure the CA trustpoint.

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint ca-name
RP/0/RP0/CPU0:router(config-trustp)# enrollment url ca-URL
RP/0/RP0/CPU0:router(config-trustp)# rsakeypair keypair-label (This command must be completed if a
keypair label is specified in Step 2.)
RP/0/RP0/CPU0:router(config-trustp)# exit
RP/0/RP0/CPU0:router(config)# commit
```

The following example is shown:

```
RP/0/RP0/CPU0:router(config)# crypto ca trustpoint myca
RP/0/RP0/CPU0:router(config-trustp)# enrollment url http://myca/mydomain.com
RP/0/RP0/CPU0:router(config-trustp)# rsakeypair keypair-label
RP/0/RP0/CPU0:router(config-trustp)# exit
RP/0/RP0/CPU0:router(config)# commit
```

Step 5 Exit configuration mode.

```
RP/0/RP0/CPU0:router(config)# commit
```

Step 6 Authenticate the CA by getting the certificate for the CA.

```
RP/0/RP0/CPU0:router# crypto ca authenticate ca-name
```

Step 7 Obtain a router certificate from the CA.

```
RP/0/RP0/CPU0:router# crypto ca enroll ca-name
```

Step 8 Verify that the router was granted a certificate. This command displays information about the router certificate and the CA certificate.

```
RP/0/RP0/CPU0:router# show crypto ca certificate
```

Enabling the Secure HTTP Server and XML Agent

To enable the secure HTTP server and XML agent, perform the following steps:

Step 1 Establish a secure session with the router.

Step 2 Enter configuration mode.

```
RP/0/RP0/CPU0:router# configure
```

Step 3 Enable the HTTPS server on the router.

```
RP/0/RP0/CPU0:router(config)# http server ssl
```



Note If you are using either serial or terminal server connection modes, go to step6.

Step 4 Enable the SSH server.

```
RP/0/RP0/CPU0:router(config)# ssh server enable
```

Step 5 Enable the XML agent with SSL.

For CORBA XML agent:

```
RP/0/RP0/CPU0:router(config)# xml agent corba ssl
```

For TTY XML agent:

```
RP/0/RP0/CPU0:router(config)# xml agent tty
```

Step 6 Exit configuration mode.

```
RP/0/RP0/CPU0:router(config)# commit
```

Testing the CWI Client

Verify that you can connect to the router by logging in to the router. See the “Starting the CWI” section on page 12 for procedures. If you are unable to log in to the router, see the “Troubleshooting Basic IP Connectivity” section on page 11.

Troubleshooting Basic IP Connectivity

This section provides information on troubleshooting basic IP connectivity problems when attempting to log in to a router using the CWI.

If you are unable to connect to the router HTTP server using the browser, follow these steps in sequence, exiting the test steps when a failure is encountered.

Step 1 Ping the IP address of the router management Ethernet interface from the client PC/workstation.

If this step fails, the problem can be an incorrect IP address, incorrect management Ethernet interface configuration, or a network connectivity problem.

Step 2 (Optional) Ping the DNS name of the router.

If this step fails, the problem is an incorrect hostname to IP address mapping. See the “Router Prerequisites” section on page 7.

Step 3 Check that the HTTP Server is running on the router using the following command:

```
RP/0/RP0/CPU0:router# show process emweb
```

If this step fails, start the HTTP server. See Step 3 in the “Setting Up the Required Management Services Without a Secure Connection” section on page 8 or Step 3 in the “Setting Up the Required Management Services with a Secure Connection” section on page 8.

If you are unable to log in to the router from the CWI login screen, run the Troubleshooter application at the prompt. See the *Cisco Craft Works Interface User Interface Guide* for information on using the Troubleshooter application.

5 Getting Started with the CWI

This section describes the procedures for establishing a connection between the CWI and a router. The procedures are described in the following sections:

- CWI Login Information Requirements, page 11
- Starting the CWI, page 12
- Logging In to Multiple Logical Routers, page 17
- Logging Out of a Logical Router, page 18
- Closing the CWI, page 20

When starting the CWI and logging in to a router, you always log in to a single router. After you have logged in to a single router, you can log in to and manage multiple routers, but you must log in to each one separately. Each router appears in the CWI Desktop Inventory Tree. For more information, see “CWI Desktop Window” section on page 21.

CWI Login Information Requirements

Contact your system administrator to obtain the following information required to complete the procedures in this section:

- The hostnames (DNS names) or IP addresses of any routers you want to log in to.
- Valid username and password for each router you want to log in to using the CWI. The username and password for each router is your AAA username and password for that router. Therefore, each router may have a different username and password.



Note The Telnet/SSH server must be enabled before you can manage a router using certain CWI features. These features include the Telnet/SSH application, the Troubleshooter application, setting character displays in the Rack View application, and viewing committed configuration changes using the Configuration Change dialog box. See the *Cisco IOS XR System Security Configuration Guide* for information on enabling the Telnet/SSH server.



Note If you are using the CORBA connections and require notifications, the router must be explicitly configured for each client that is to receive notifications. These notifications include real-time inventory updates (for example online insertion and removal [OIR]), alarms, and change of configuration events. See the “Router Prerequisites” section on page 7 for information on configuring the router to send notifications to a specified client.

Starting the CWI

The following two sections provide procedures for starting the CWI and logging in to a router:

- Starting the CWI When SSL Is not Enabled, page 12
- Starting the CWI When SSL Is Enabled, page 14

Starting the CWI When SSL Is not Enabled

Use this procedure to start the CWI and log in to a router when SSL is not enabled on the required Management Services. See the “Setting Up the Required Management Services Without a Secure Connection” section on page 8.

To start the CWI when SSL is not enabled, perform the following steps.

-
- Step 1** Start a supported web browser. See the “CWI Client System Prerequisites” section on page 5 for information on web browsers.
- The web browser window appears.
- Step 2** In the Address field located near the top of the web browser window, enter the DNS name or IP address of the router to be accessed.
- You must enter the DNS name or IP address in Address field using the following format:
- `http://router-dns-name` or `http://ip-address`
- Step 3** Press Enter.
- Step 4** A router HTTP authentication dialog box appears.
- You require your AAA username and password. See the *Cisco IOS XR Getting Started Guide* for information on the AAA username and password.
- a. Enter your AAA username and password in the User Name and Password fields.
 - b. Click OK.
- The Cisco Systems router homepage appears.
- Step 5** Click the **Craft Works Interface** link in the web browser.
- Step 6** A router HTTP authentication dialog box appears.
- Your AAA username and password must be provided for the Craft Works Interface Launcher to start. See the *Cisco IOS XR Getting Started Guide* for information on the AAA username and password.
- a. Enter the same AAA username and password that you used in Step 4 in the User Name and Password fields.
 - b. Click Yes.
- Step 7** If this is the first time the CWI client has started the CWI, the Java Plug-in must be installed and the CWI Cisco security certificate must be accepted.
- a. If the Java Plug-in installation is completed, a dialog box appears asking you to trust the security certificate distributed by Cisco Systems, Inc. This dialog box will differ depending on the client platform.

- b. The security certificate must be accepted to run CWI. You have the following options:
- Click **Yes** to trust and accept the security certificate for this router session only. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 9.
 - Click **No** to deny the security certificate. If this option is chosen, the login process is canceled.
 - Click **Always** to automatically trust and accept the security certificate in this section and all subsequent CWI sessions. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 8.
 - Click **More Details** to view the security certificate. A dialog box appears with detailed certificate information. The certificate information includes the version, serial number, insurer, and start and end date validity of the certificate.

If applicable, the Craft Works Interface Launcher appears.

Step 8 If this is the first time you have started the CWI or if you have installed a new version of the CWI, the CWI components will start downloading. Otherwise, a cached version of the CWI components are used, reducing the CWI start time.

After the CWI component download is complete, the Start CWI, Delete Cache, and About buttons become available.

Step 9 Log in to the router when the CWI - Login dialog box appears (see Figure 2).



Note Enter the same AAA username and password that you used in Step 4 to access the router that must be configured. See the “Router Prerequisites” section on page 7.

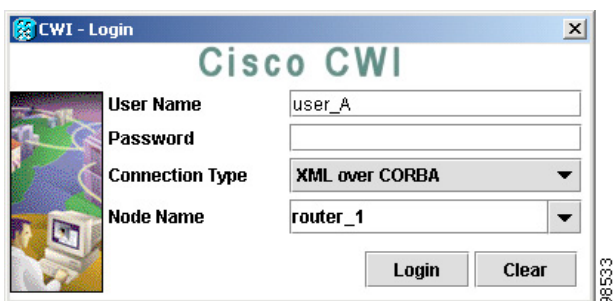
- Enter the same AAA username that you used in Step 4 in the User Name field. See the “CWI Login Information Requirements” section on page 11 for information on obtaining your username.
- Enter the same AAA password that you used in Step 4 in the Password field. See the “CWI Login Information Requirements” section on page 11 for information on obtaining your password.
- Choose one of the following connection types from the drop-down menu:



Note CWI can autodetect whether the router is configured in secure or nonsecure mode and will try the different standard ports as necessary.

- XML over CORBA. Choose the Node Name.
 - CLI over Telnet/SSH. Choose the ServerName/Port. If you specify a port, CWI will try only to connect using that port. CWI will not automatically try to connect with other ports.
 - Terminal Server. Choose the ServerName/Port.
 - Serial Port. Choose the Serial Port. You can also set the parameters for the serial port.
- (Optional) In the Node Name list, click the drop-down arrow and choose a node name (DNS name or IP address of the router).
 - Click Login.

Figure 2 CWI - Login Dialog Box



Step 10 Observe the dynamic display that shows each initialization step and indicates whether each step is successful.

After the CWI initialization is complete, the CWI Desktop window appears. See the “CWI Desktop Window” section on page 21 for information on the CWI Desktop window.



Note The CWI is automatically locked when there is no activity in the CWI session for 15 minutes. To unlock the CWI, you must provide the username and password used when logging in to the router. See the *Cisco Craft Works Interface User Interface Guide* for CWI unlocking procedures.

If any of the minimum requirements of the initialization steps fail, a CWI dialog box appears allowing you to Abort, Troubleshoot, or Continue the initialization process.

Step 11 If necessary, complete the following steps to troubleshoot the initialization process.

- a. To stop the initialization process, click **Abort**.
- b. To troubleshoot the process, click **Troubleshoot**. The Troubleshooter application is started, and a Troubleshoot New LR Launch problems dialog box appears. The Troubleshooter application allows you to run fault isolation tests on the client/server communication path between the CWI and the router management agent. The Troubleshooter application provides a window that describes the reason for the failure, possible cause, and recommended repair action. An automatic repair option is provided in many instances. See the *Cisco Craft Works Interface User Interface Guide* for information on using the Troubleshooter feature.
- c. To continue the initialization process, click **Continue**.

Starting the CWI When SSL Is Enabled

Use this procedure to start the CWI and log in to a router when SSL is enabled on the required Management Services. See the “Setting Up the Required Management Services with a Secure Connection” section on page 8 for information on enabling SSL.



Note All steps associated with accepting a certificate are not required after the first time you have started the CWI client and logged in to a router if you choose the certificate option Always. See the “Starting the CWI When SSL Is not Enabled” section on page 12 for procedures to start the CWI and log in to a router for a subsequent log in.

To start the CWI when SSL is enabled, perform the following steps.

Step 1 Start a supported web browser. See the “CWI Client System Prerequisites” section on page 5 for information on web browsers.

The web browser window appears.

Step 2 In the Address field located near the top of the web browser window, enter the DNS name or IP address of the router to be accessed.

You must enter the DNS name or IP address in Address field using the following format:

`https://router-dns-name` or `https://ip-address`

Step 3 Press **Enter**.

Step 4 The router SSL certificate must be accepted.



Note If you click **No** to deny the SSL certificate, the login process is canceled.

You have the following options:

- Click **Yes** to trust and accept the SSL certificate for this router session only. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 5. If you choose Yes, the SSL certificate must be accepted next time you log in to the router.
- Click **Always** to automatically trust and accept the SSL certificate in this session and all subsequent CWI sessions. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 5. If you choose Always, the SSL certificate does not have to be accepted again when logging in to a router from the CWI client.

- Click **More Details** to view the SSL certificate. A dialog box appears with detailed certificate information. The certificate information includes the version, serial number, insurer, and start and end date validity of the certificate.

Step 5 A router HTTP authentication dialog box appears.

You require your AAA username and password. See the *Cisco IOS XR Getting Started Guide* for information on the AAA username and password.

- Enter your AAA username and password in the User Name and Password fields.
- Click **OK**.

The Cisco Systems router homepage appears.

Step 6 Click the **Craft Works Interface** link in the web browser.

Step 7 A router HTTP authentication dialog box appears.

Your AAA username and password must be provided for the Craft Works Interface Launcher to start. See the “Router Prerequisites” section on page 7 for information on the AAA username and password.

- Enter your AAA username and password in the User Name and Password fields.
- Click **Yes**.

Step 8 If this is the first time the CWI client has started the CWI, the Java Plug-in must be installed and the CWI Cisco security certificate must be accepted.

- If the Java Plug-in installation is completed, a dialog box appears asking you to trust the security certificate distributed by Cisco Systems, Inc.
- The security certificate must be accepted to run CWI. You have the following options:
 - Click **Yes** to trust and accept the security certificate for this router session only. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 9.
 - Click **No** to deny the security certificate. If this option is chosen, the login process is canceled.
 - Click **Always** to automatically trust and accept the security certificate in this section and all subsequent CWI sessions. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 9.
 - Click **More Details** to view the security certificate. A dialog box appears with detailed certificate information. The certificate information includes the version, serial number, insurer, and start and end date validity of the certificate.

Step 9 The router SSL certificate must be accepted.



Note

If you click **No** to deny the SSL certificate, the login process is canceled.

You have the following options:

- Click **Yes** to trust and accept the SSL certificate for this router session only. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 10.
- Click **Always** to automatically trust and accept the SSL certificate in this session and all subsequent CWI sessions. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 10.
- Click **More Details** to view the SSL certificate. A dialog box appears with detailed certificate information. The certificate information includes the version, serial number, insurer, and start and end date validity of the certificate.

If you choose either the Yes or Always options, the Craft Works Interface Launcher appears.

Step 10 If this is the first time you have started the CWI or if you have installed a new version of the CWI, the CWI components will start downloading. Otherwise, a cached version of the CWI components are used, reducing the CWI start time.

After the CWI component download is complete, the Start CWI, Delete Cache, and About buttons become available.

Step 11 Log in to the router when the CWI - Login dialog box appears (see Figure 2).



Note A valid AAA username and password for accessing the router must be configured. See the “Router Prerequisites” section on page 7.

- a. Enter a username in the User Name field. See the “CWI Login Information Requirements” section on page 11 for information on obtaining your username.
- b. Enter a password in the Password field. See the “CWI Login Information Requirements” section on page 11 for information on obtaining your password.
- c. Choose one of the following connection types from the drop-down menu:



Note CWI can autodetect whether the router is configured in secure or nonsecure mode and will try the different standard ports as necessary.

- XML over CORBA. Choose the Node Name.
 - CLI over Telnet/SSH. Choose the ServerName/Port. If you specify a port, CWI will try only to connect using that port. CWI will not automatically try to connect with other ports.
 - Terminal Server. Choose the ServerName/Port.
 - Serial Port. Choose the Serial Port. You can also set the parameters for the serial port.
- d. (Optional) In the Node Name list, click the drop-down arrow and choose a node name (DNS name or IP address of the router).
 - e. Click **Login**.

Step 12 If you did not choose Always in Step 9, you must accept the SSL certificate.



Note If you click **No** to deny the SSL certificate, the login process is canceled.

You have the following options:

- Click **Yes** to trust and accept the SSL certificate for this router session only. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 13.
- Click **Always** to automatically trust and accept the SSL certificate in this session and all subsequent CWI sessions. If this option is chosen, the certificate is accepted and the login process continues. Proceed to Step 13.
- Click **More Details** to view the SSL certificate. A dialog box appears with detailed certificate information. The certificate information includes the version, serial number, insurer, and start and end date validity of the certificate.

If you choose either the Yes or Always options, the Initializing CWI dialog box appears.

Step 13 Observe the dynamic display that shows each initialization step and indicates whether each step is successful.

When the CWI initialization is complete, the CWI Desktop window appears. See the “CWI Desktop Window” section on page 21 for information on the CWI Desktop window.

**Note**

The CWI is automatically locked when there is no activity in the CWI session for 15 minutes. To unlock the CWI you must provide the username and password used when logging in to the router. See the *Cisco Craft Works Interface User Interface Guide* for CWI unlocking procedures.

If any of the minimum requirements of the initialization steps fail, a CWI dialog box appears allowing you to Abort, Troubleshoot, or Continue the initialization process. Proceed to Step 14.

Step 14 If necessary, complete the following steps to troubleshoot the initialization process.

- a. To stop the initialization process, click **Abort**.
 - b. To troubleshoot the process, click **Troubleshoot**. The Troubleshooter application is started, and a Troubleshoot New LR Launch problems dialog box appears. The Troubleshooter application allows you to run fault isolation tests on the client/server communication path between the CWI and the router management agent. The Troubleshooter application provides a window that describes the reason for the failure, possible cause, and recommended repair action. An automatic repair option is provided in many instances. See the *Cisco Craft Works Interface User Interface Guide* for information on using the Troubleshooter feature.
 - c. To continue the initialization process, click **Continue**.
-

Logging In to Multiple Logical Routers

The CWI can manage multiple routers. You can log in to multiple routers when the CWI Desktop is open and currently logged in to at least one router.

To log in to a router from the CWI Desktop, perform the following steps:

Step 1 Choose **File > Login**.

The CWI - Login dialog box appears (see Figure 2).

Step 2 In the User Name field, enter a valid username. See the “CWI Login Information Requirements” section on page 11 for information on obtaining your username.

Step 3 In the Password field, enter a valid password. See the “CWI Login Information Requirements” section on page 11 for information on obtaining your password.

**Note**

A valid AAA username and password for accessing the router must be configured. See the *Cisco IOS XR Getting Started Guide* for information on configuring usernames and passwords on the router.

Step 4 In the Node Name field, enter a valid node name (DNS name or IP address of the router) or click the drop-down arrow and choose a valid node name.

Step 5 Click **Login**.

Step 6 If this is the first time the router has started from the CWI client and the required Management Services are running SSL, a certificate dialog box appears. The Cisco security certificate must be accepted to log in to the router.

**Note**

If you click **No** to deny the SSL certificate, the login process is canceled.

You have the following options:

- a. Click **Yes** to trust and accept the security certificate for this router session only. If this option is chosen, the certificate is accepted and the login process continues.
- b. Click **Always** to automatically trust and accept the security certificate in this section and all subsequent sessions with this specific router from the CWI client. If this option is chosen, the certificate is accepted and the login process continues.

- c. Click **More Details** to view the security certificate. A dialog box appears with detailed certificate information. The certificate information includes the version, serial number, insurer, and start and end date validity of the certificate.

If you choose either the Yes or Always options, the Initializing CWI dialog box appears.

After the router initialization is successfully completed, a new router appears in the Inventory Tree in the CWI Desktop. See the CWI Desktop Window, page 21 for information on the Inventory Tree.

Logging Out of a Logical Router

You can log out of a router when there is more than one router open in the CWI Desktop.



Note You must commit any uncommitted changes that you want to keep.

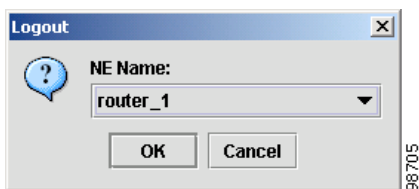
To log out of a router, perform the following steps:

Step 1 Choose a router in the Inventory Tree.

Step 2 Choose **File > Logout**.

A Logout dialog box appears (see Figure 3).

Figure 3 Logout Dialog Box

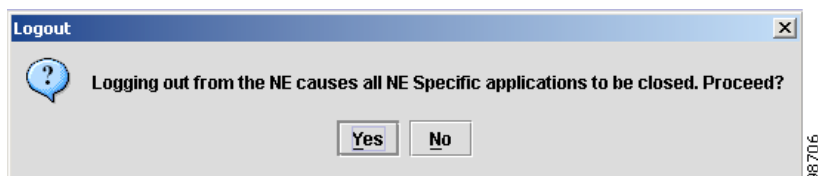


Step 3 Choose a router from the NE Name list.

Step 4 Click **OK**.

A second Logout dialog box appears to confirm that you want to log out of the router (see Figure 4).

Figure 4 Logout Dialog Box



Step 5 Click **Yes**.

All applications opened from the selected router are closed, the session with the router is ended, and the router disappears from the Inventory Tree. See the CWI Desktop Window, page 21 for information on the Inventory Tree.

6 Locking and Unlocking the CWI

The CWI can be manually locked; otherwise, it is automatically locked when there is no activity in the CWI for 15 minutes. Locking the CWI prevents unauthorized users from accessing the CWI. A valid user password is required to unlock the CWI.

The following procedures to lock and unlock a CWI session are provided:

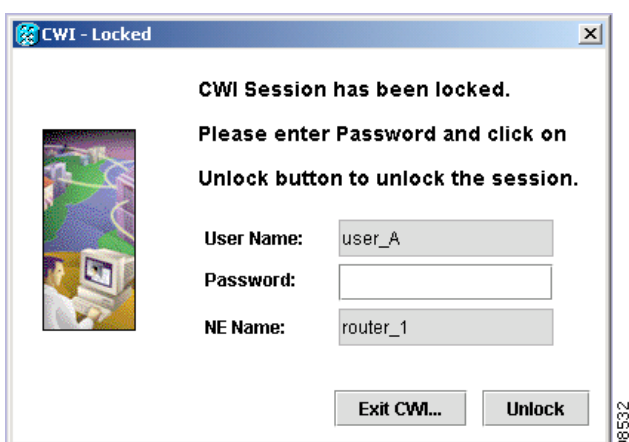
- Manually Locking the CWI, page 19
- Unlocking the CWI, page 19

Manually Locking the CWI

From the CWI Desktop, choose **File > Lock** to manually lock the CWI. For information on the CWI Desktop and CWI Desktop menus, see the *Cisco Craft Works Interface User Interface Guide*.

When the CWI is locked, a CWI - Locked dialog box appears (see Figure 5).

Figure 5 CWI - Locked Dialog Box



Unlocking the CWI

To unlock the CWI, perform the following steps:

-
- Step 1** In the Craft Works Interface - Locked dialog box (see Figure 5), enter a valid password in the Password field. See the “Router Prerequisites” section on page 7 for information on obtaining your password.
 - Step 2** Click **Unlock**.
 - Step 3** Click **Exit CWI** to close the CWI application.
The Craft Works Interface - Locked dialog box closes and the CWI is unlocked.
-

7 Installing and Accessing Online Help

The first time the CWI Desktop is opened, the online help should be installed. The online help provides a descriptive overview of the windows, menu items, toolbar buttons, status icons, and other interface features of the CWI that can be launched from the CWI Desktop Help menu. For information on the CWI Desktop Help menu, see the *Cisco Craft Works Interface User Interface Guide*.

To install the CWI Online Help, perform the following steps:

- Step 1

In the CWI Desktop, choose **Help > Help Desktop**.
A Help dialog box appears.
- Step 2

Click **Yes** to install Help.
An Online Help Installer dialog box appears and downloads the help files.
When the download is complete, a CWI Help installation complete message appears in the dialog box.
- Step 3

Click **Close**.
The Online Help Installer dialog box closes.
- Step 4

To access the online help, choose **Help > Help Desktop** to open the online help.

8 Closing the CWI



Note You must commit any uncommitted changes that you want to keep.

To close the CWI, perform the following steps:

- Step 1

Choose **File> Exit**. Or click **Close** on the CWI Desktop title bar.
A Craft Works Interface dialog box appears.
- Step 2

Click **Yes** to exit the application.
The CWI Desktop window closes. The Configuration Desktop is also closed (if it was open when the close command was executed).

9 CWI Supported Connection Methods and Applications

Table 6 provides detailed information on the supported CWI connections methods and available applications.



Note If you are connecting to the router through either the Terminal Server or Serial Port connection methods from CWI, you must ensure that the logging console is not configured on the router.

Table 6 Connection Methods and Applications

CWI Application	Console Port (serial cable or through a terminal server)	Telnet (no XML)	Telnet, or CORBA connection (XML)
Launch/Login	Yes. Enter the serial port or terminal server/port name.	Yes. Enter the DNS name or IP address.	Yes. Enter the DNS name or IP address.
Main Desktop	Yes, but no notifications or associated alarms are displayed.	Yes, but no notifications or associated alarms are displayed.	Yes
Alarm Viewer	Yes, but no alerts are displayed.	Yes, but no alerts are displayed.	Yes
Alarm Dashboard	—	—	Yes
Inventory Viewer	Yes	Yes	Yes

Table 6 **Connection Methods and Applications (continued)**

CWI Application	Console Port (serial cable or through a terminal server)	Telnet (no XML)	Telnet, or CORBA connection (XML)
Interface Viewer	Yes	Yes	Yes
Rack View	Yes, but no notifications and associated alarms are displayed.	Yes, but no notifications and associated alarms are displayed.	Yes
Telnet Plus/SSH Plus	—	Yes	Yes
Terminal Plus	Yes, but mutually exclusive to other applications. ¹	—	—
Troubleshooter	—	—	Yes
Configuration Desktop ²	—	—	Yes
Configuration Editor	Yes	Yes	Yes
Graphical Configuration	—	—	Yes

1. When connecting through the serial port or terminal server, the terminal application requires exclusive access to the connection, so no other applications can be launched or refreshed while it is open.

2. The Configuration Desktop is available only when using XML connection type, for example, XML over CORBA.

10 CWI Desktop Window

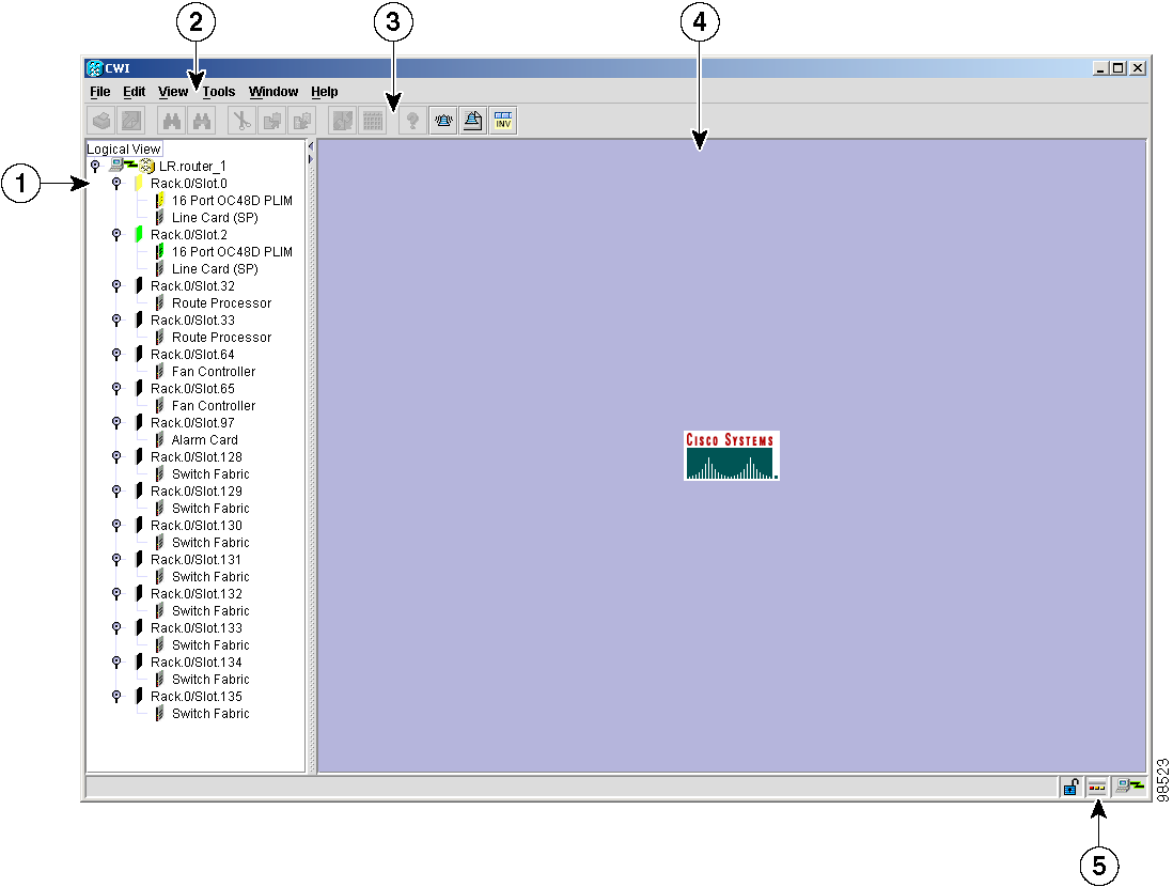
The CWI Desktop is the main point of access to all CWI applications and tools, allowing you to configure, monitor, and manage routers (see Figure 6).

The CWI Desktop is designed with common elements that provide an easy to use and consistent user interface. The elements of the CWI Desktop window are described in Table 7.

Table 7 **CWI Desktop Window Elements**

Element	Description
Menu Bar	Provides a list of options available on the basis of the selected object and active application. The options include administrative, editing, viewing tasks, starting applications, and arranging windows.
Toolbar	Contains icons, referred to as tools, that provide direct access to context-sensitive functions. Clicking a tool selects a task.
Inventory Tree	Displays all components of each router that the CWI can access and is the primary interface to these components. The Inventory Tree dynamically shows current alarms and events, connectivity status, and physical and logical tree views. The Inventory Tree provides context-sensitive launching of applications by selecting an object, a group of objects, or an entire router in the Inventory Tree and then choosing an available application
CWI Status Bar	Contains three icons that show the status of the CWI including communication security and NE connectivity and allows you to open the Alarm Dashboard. The left side of the status bar may contain a progress message.
Dashboard	Provides a summary of the alarm status information for all routers in the CWI Desktop. Color coding is used to indicate active alarm counts by severity. A resettable running count of new alarm arrivals is provided.
CWI Application Pane	Contains the active CWI applications that are used to manage the router. Multiple applications can be opened concurrently in the CWI Application pane.

Figure 6 CWI Desktop



1	Inventory Tree	4	CWI Application Pane
2	CWI Desktop Menu Bar	5	CWI Desktop Status Bar
3	CWI Desktop Toolbar	—	—

The CWI Desktop allows you to communicate with the router using the applications that are described in Table 8.

Table 8 List of Applications for the CWI Desktop

Name of Application	Description
Alarm Viewer	Provides an interface between the CWI and the alarm management functions of the router controller, allowing you to dynamically view alarm records with powerful filtering capabilities. The Alarm Viewer also provides a launch point to view correlated alarms.
Inventory Viewer	Displays the attribute values of selected objects.
Rack View	Displays a graphical representation of the physical equipment including racks, cards, slots, power supplies, and fan trays. The router can be viewed from the front or the back. The Rack View displays active alarms on the associated object and provides context-sensitive launch points for other CWI applications in the same way as the Inventory Tree. The card character displays are user configurable and are displayed on the card faceplate.
Interface Viewer	Provides a view of interface attributes for selected cards.

Table 8 **List of Applications for the CWI Desktop (continued)**

Name of Application	Description
Configuration Desktop	Provides an interface tailored to managing configuration applications. See “Configuration Desktop Window” section on page 23 for more information about the Configuration Desktop window.
Telnet/SSH/Terminal Plus	Provides the capability to issue CLI commands and view session information within the CWI. Telnet/SSH/Terminal Plus include additional CWI features for creating command lists and running commands from the command list, saving and loading command lists from a file, and running in batch mode. Additionally, console text can be displayed in a separate window. The SSH application connects to the router with a secure connection.
Troubleshooter	Provides fault isolation and repair of connectivity problems between the CWI and router.
Configuration Editor	Displays the target configuration in CLI format. The Configuration Editor provides general text editor functions such as copy, paste, redo, and undo, and provides syntax checking and CLI functions such as command completion and CLI help.

11 Configuration Desktop Window

The Configuration Desktop is the main point of access to all configuration applications (see Figure 7). These applications configure and manage routers within your network.

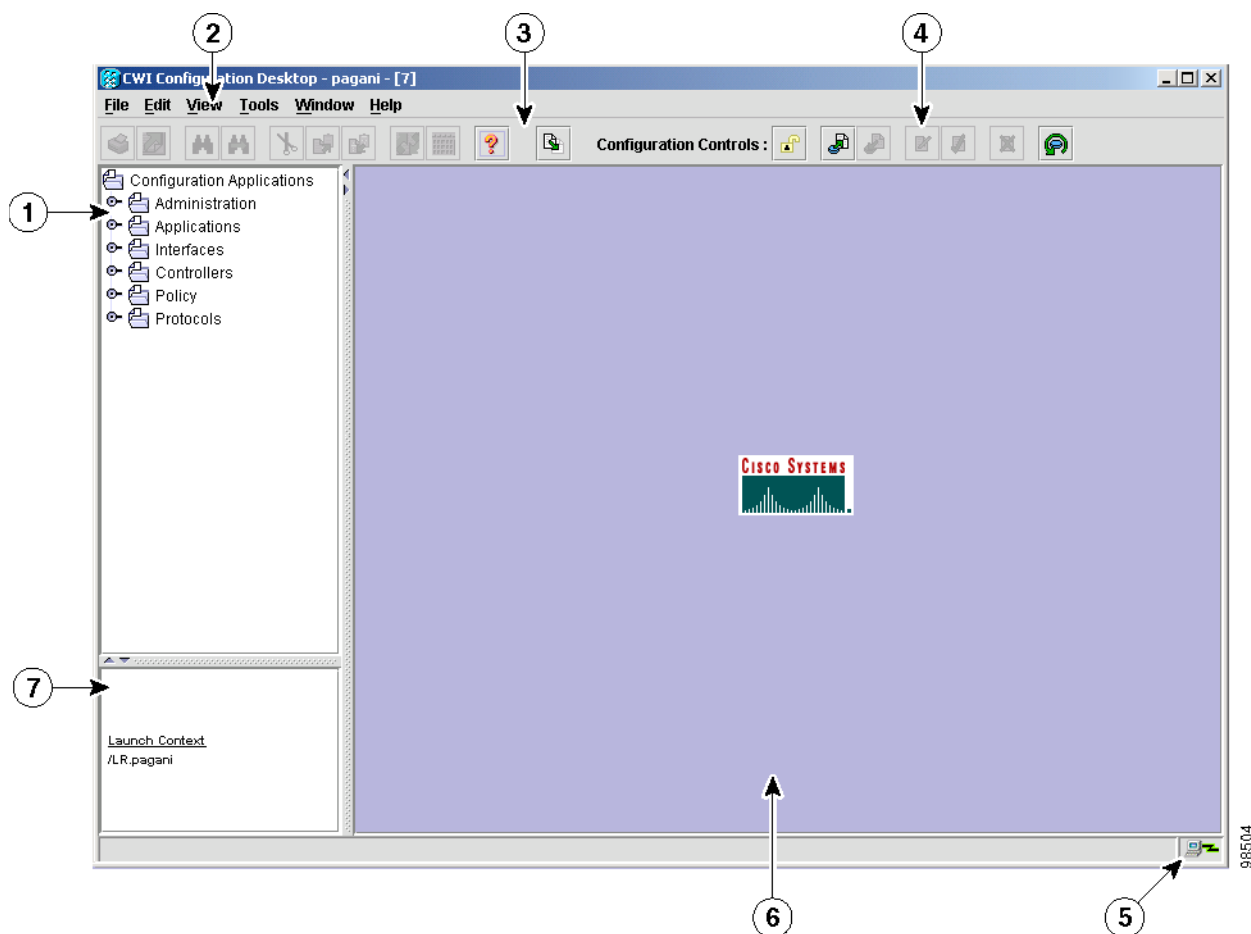
The Configuration Desktop is opened for one router chosen in the CWI Desktop. If there are multiple routers in the CWI Desktop, you can open one Configuration Desktop for each router.

The Configuration Desktop window elements are described in Table 9.

Table 9 **Configuration Desktop Window Elements**

Element	Description
Configuration Desktop Menu Bar	Provides a list of options that are available based on the chosen object and active application. The options are administrative, editing, and viewing tasks; starting applications; and arranging windows.
Configuration Desktop Toolbar	Contains tools representing commonly used tasks in the Configuration Desktop. The toolbar provides quick access to common tasks used in all the configuration applications, allows you to open the Replace Configuration Editor, and controls the committing of a target configuration to the running configuration.
Configuration Applications Tree	Uses icons for each configuration application to dynamically display the state of each application. The icon states include the unchanged, not permitted, incompatible version, uncommitted, and disabled states.
Launch Context Pane	Displays the components available to be configured (the launch point from the CWI Desktop).
Configuration Applications Pane	Contains the active configuration applications that are used to configure the router. Multiple applications can be opened concurrently in the Configuration Applications pane.
Configuration Desktop Status Bar	Provides information on the status of the Configuration Desktop.

Figure 7 Configuration Desktop



1	Configuration Applications Tree	5	Configuration Desktop status bar
2	Configuration Desktop menu bar	6	Configuration Applications pane
3	Configuration Desktop toolbar (Standard toolbar icons)	7	Launch Context pane
4	Configuration Desktop toolbar (Configuration Controls toolbar icons)	—	—

There are four ways to configure a router using the CWI:

- Telnet/SSH/Terminal Plus application from the CWI Desktop.
- Configuration Editor from the CWI Desktop.
- Replace Configuration Editor from the Configuration Desktop.
- Graphical user interface (GUI) applications from the Configuration Desktop.

The Configuration Desktop allows you to view the configuration changes made using the configuration applications or the Configuration Editor (from the CWI Desktop) using the View Uncommitted Configuration tool. You can click the View Uncommitted Configuration icon from the Configuration Desktop. The uncommitted configuration (also known as the target configuration) is displayed in a window in CLI format.

A two-stage running configuration commit functionality, which includes locking, abort, commit, and rollback control, is provided in the Configuration Desktop.

See the *Cisco Craft Works Interface User Interface Guide* for detailed information on the Configuration Desktop.

Common Elements in the Configuration Desktop

The graphical configuration applications launched from the Configuration Desktop include a common feature set. These features include bulk configuration and validation. The bulk configuration features provide “templating without templates.” These features include the capability to take an existing configured object and utilize user selected attributes as a template for configuring one or more additional objects.

Other common features include:

- Cloning the selected attributes of a record to create new records containing the attributes of the original record. In addition, you can apply an algorithm that generates values of selected key fields.
- Copying and pasting one or more selected attributes from one record to one or more records.
- Editing a single attribute across multiple rows in a table with a single operation.
- Client-side field validation.
- Client-and server-side error checking.
- Resequencing records.

The Configuration Desktop provides the following GUI applications:

- Administration Configuration: AAA, Alarm Administration, and User Administration.
- Applications Configuration: IEP and MPLS-TE.
- Interfaces Configuration: Common, Ethernet, and PoS.
- Controllers Configuration: SONET.
- Policy Configuration: Access Control Lists, Packet Filter, QoS, and Routing Policy.
- Protocols Configuration: BGP, ISIS, LDP, OSPF, and RSVP.

You can concurrently access multiple applications within the Configuration Desktop.

Replace Configuration Editor

The Replace Configuration Editor application is available in the Configuration Desktop and allows you to replace the running configuration on the router with the contents of the Replace Configuration Editor window.

The Replace Configuration Editor provides general text editor functions such as copy, paste, redo, and undo, and provides syntax checking and CLI functions such as command completion and CLI help.

12 Obtaining Documentation

Cisco documentation and additional literature are available on Cisco.com. Cisco also provides several ways to obtain 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 at this URL:

<http://www.cisco.com/techsupport>

You can access the Cisco website at this URL:

<http://www.cisco.com>

You can access international Cisco websites at this URL:

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

Product Documentation DVD

Cisco documentation and additional literature are available in the Product Documentation DVD package, which may have shipped with your product. The Product Documentation DVD is updated regularly and may be more current than printed documentation.

The Product Documentation DVD is a comprehensive library of technical product documentation on portable media. The DVD enables you to access multiple versions of hardware and software installation, configuration, and command guides for Cisco products and to view technical documentation in HTML. With the DVD, you have access to the same documentation that is found on the Cisco website without being connected to the Internet. Certain products also have .pdf versions of the documentation available.

The Product Documentation DVD is available as a single unit or as a subscription. Registered Cisco.com users (Cisco direct customers) can order a Product Documentation DVD (product number DOC-DOCDVD=) from Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Ordering Documentation

Beginning June 30, 2005, registered Cisco.com users may order Cisco documentation at the Product Documentation Store in the Cisco Marketplace at this URL:

<http://www.cisco.com/go/marketplace/>

Nonregistered Cisco.com users can order technical documentation from 8:00 a.m. to 5:00 p.m. (0800 to 1700) PDT by calling 1 866 463-3487 in the United States and Canada, or elsewhere by calling 011 408 519-5055. You can also order documentation by e-mail at tech-doc-store-mkpl@external.cisco.com or by fax at 1 408 519-5001 in the United States and Canada, or elsewhere at 011 408 519-5001.

13 Documentation Feedback

You can rate and provide feedback about Cisco technical documents by completing the online feedback form that appears with the technical documents on Cisco.com.

You can send comments about Cisco documentation 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.

14 Cisco Product Security Overview

Cisco provides a free online Security Vulnerability Policy portal at this URL:

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

From this site, you can perform these tasks:

- Report security vulnerabilities in Cisco products.
- Obtain assistance with security incidents that involve Cisco products.
- Register to receive security information from Cisco.

A current list of security advisories and notices for Cisco products is available at this URL:

<http://www.cisco.com/go/psirt>

If you prefer to see advisories and notices as they are updated in real time, you can access a Product Security Incident Response Team Really Simple Syndication (PSIRT RSS) feed from this URL:

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

Reporting Security Problems in Cisco Products

Cisco is committed to delivering secure products. We test our products internally before we release them, and we strive to correct all vulnerabilities quickly. If you think that you might have identified a vulnerability in a Cisco product, contact PSIRT:

- Emergencies—security-alert@cisco.com

An emergency is either a condition in which a system is under active attack or a condition for which a severe and urgent security vulnerability should be reported. All other conditions are considered nonemergencies.

- Nonemergencies—psirt@cisco.com

In an emergency, you can also reach PSIRT by telephone:

- 1 877 228-7302
- 1 408 525-6532



Tip

We encourage you to use Pretty Good Privacy (PGP) or a compatible product to encrypt any sensitive information that you send to Cisco. PSIRT can work from encrypted information that is compatible with PGP versions 2.x through 8.x.

Never use a revoked or an expired encryption key. The correct public key to use in your correspondence with PSIRT is the one linked in the Contact Summary section of the Security Vulnerability Policy page at this URL:

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

The link on this page has the current PGP key ID in use.

15 Obtaining Technical Assistance

Cisco Technical Support provides 24-hour-a-day award-winning technical assistance. The Cisco Technical Support & Documentation website on Cisco.com features extensive online support resources. In addition, if you have a valid Cisco service contract, Cisco Technical Assistance Center (TAC) engineers provide telephone support. If you do not have a valid Cisco service contract, contact your reseller.

Cisco Technical Support & Documentation Website

The Cisco Technical Support & Documentation website provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The website is available 24 hours a day, at this URL:

<http://www.cisco.com/techsupport>

Access to all tools on the Cisco Technical Support & Documentation website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a user ID or password, you can register at this URL:

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



Note

Use the Cisco Product Identification (CPI) tool to locate your product serial number before submitting a web or phone request for service. You can access the CPI tool from the Cisco Technical Support & Documentation website by clicking the **Tools & Resources** link under Documentation & Tools. Choose **Cisco Product Identification Tool** from the Alphabetical Index drop-down list, or click the **Cisco Product Identification Tool** link under Alerts & RMAs. The CPI tool offers three search options: by product ID or model name; by tree view; or for certain products, by copying and pasting **show** command output. Search results show an illustration of your product with the serial number label location highlighted. Locate the serial number label on your product and record the information before placing a service call.

Submitting a Service Request

Using the online TAC Service Request Tool is the fastest way to open S3 and S4 service requests. (S3 and S4 service requests are those in which your network is minimally impaired or for which you require product information.) After you describe your situation, the TAC Service Request Tool provides recommended solutions. If your issue is not resolved using the recommended resources, your service request is assigned to a Cisco engineer. The TAC Service Request Tool is located at this URL:

<http://www.cisco.com/techsupport/servicerequest>

For S1 or S2 service requests or if you do not have Internet access, contact the Cisco TAC by telephone. (S1 or S2 service requests are those in which your production network is down or severely degraded.) Cisco engineers are assigned immediately to S1 and S2 service requests to help keep your business operations running smoothly.

To open a service request by telephone, use one of the following numbers:

Asia-Pacific: +61 2 8446 7411 (Australia: 1 800 805 227)

EMEA: +32 2 704 55 55

USA: 1 800 553-2447

For a complete list of Cisco TAC contacts, go to this URL:

<http://www.cisco.com/techsupport/contacts>

Definitions of Service Request Severity

To ensure that all service requests are reported in a standard format, Cisco has established severity definitions.

Severity 1 (S1)—Your 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.

Severity 2 (S2)—Operation of an existing network is severely degraded, or significant aspects of your business operation are negatively affected by inadequate performance of Cisco products. You and Cisco will commit full-time resources during normal business hours to resolve the situation.

Severity 3 (S3)—Operational performance of your network is impaired, but most business operations remain functional. You and Cisco will commit resources during normal business hours to restore service to satisfactory levels.

Severity 4 (S4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

16 Obtaining Additional Publications and Information

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

- Cisco Marketplace provides a variety of Cisco books, reference guides, documentation, and logo merchandise. Visit Cisco Marketplace, the company store, at this URL:
<http://www.cisco.com/go/marketplace/>
- *Cisco Press* publishes a wide range of general networking, training and certification titles. Both new and experienced users will benefit from these publications. For current Cisco Press titles and other information, go to Cisco Press at this URL:
<http://www.ciscopress.com>
- *Packet* magazine is the Cisco Systems technical user magazine for maximizing Internet and networking investments. Each quarter, Packet delivers coverage of the latest industry trends, technology breakthroughs, and Cisco products and solutions, as well as network deployment and troubleshooting tips, configuration examples, customer case studies, certification and training information, and links to scores of in-depth online resources. You can access Packet magazine at this URL:
<http://www.cisco.com/packet>
- *iQ Magazine* is the quarterly publication from Cisco Systems designed to help growing companies learn how they can use technology to increase revenue, streamline their business, and expand services. The publication identifies the challenges facing these companies and the technologies to help solve them, using real-world case studies and business strategies to help readers make sound technology investment decisions. You can access iQ Magazine at this URL:
<http://www.cisco.com/go/iqmagazine>
or view the digital edition at this URL:
<http://ciscoiq.texterity.com/ciscoiq/sample/>
- *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/ipj>
- Networking products offered by Cisco Systems, as well as customer support services, can be obtained at this URL:
<http://www.cisco.com/en/US/products/index.html>
- Networking Professionals Connection is an interactive website for networking professionals to share questions, suggestions, and information about networking products and technologies with Cisco experts and other networking professionals. Join a discussion at this URL:
<http://www.cisco.com/discuss/networking>
- World-class networking training is available from Cisco. You can view current offerings at this URL:
<http://www.cisco.com/en/US/learning/index.html>

CISCO SYSTEMS



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

European Headquarters
Cisco Systems International BV
Haarlerbergpark
Haarlerbergweg 13-19
1101 CH Amsterdam
The Netherlands
www-europe.cisco.com
Tel: 31 0 20 357 1000
Fax: 31 0 20 357 1100

Americas Headquarters
Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
www.cisco.com
Tel: 408 526-7660
Fax: 408 527-0883

Asia Pacific Headquarters
Cisco Systems, Inc.
168 Robinson Road
#28-01 Capital Tower
Singapore 068912
www.cisco.com
Tel: +65 6317 7777
Fax: +65 6317 7799

Cisco Systems has more than 200 offices in the following countries. Addresses, phone numbers, and fax numbers are listed on the

Cisco Web site at www.cisco.com/go/offices

Argentina • Australia • Austria • Belgium • Brazil • Bulgaria • Canada • Chile • China PRC • Colombia • Costa Rica • Croatia • Cyprus • Czech Republic • Denmark
Dubai, UAE • Finland • France • Germany • Greece • Hong Kong SAR • Hungary • India • Indonesia • Ireland • Israel • Italy • Japan • Korea • Luxembourg • Malaysia
Mexico • The Netherlands • New Zealand • Norway • Peru • Philippines • Poland • Portugal • Puerto Rico • Romania • Russia • Saudi Arabia • Scotland • Singapore
Slovakia • Slovenia • South Africa • Spain • Sweden • Switzerland • Taiwan • Thailand • Turkey • Ukraine • United Kingdom • United States • Venezuela • Vietnam
Zimbabwe

CCVP, the Cisco logo, and the Cisco Square Bridge logo are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn is a service mark of Cisco Systems, Inc.; and Access Registrar, Aironet, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, CCSP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, Follow Me Browsing, FormShare, GigaDrive, HomeLink, Internet Quotient, IOS, iPhone, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, iQuick Study, LightStream, Linksys, MeetingPlace, MGX, Networking Academy, Network Registrar, Packet, PIX, ProConnect, ScriptShare, SMARTnet, StackWise, The Fastest Way to Increase Your Internet Quotient, and TransPath are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the United States and certain other countries.

All other trademarks mentioned in this document or Website are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company.
0705R)

