



# Catalyst 6500 Series, 4500 Series, and 5000 Family Switches Web Interface Installation and Configuration Note

---

This installation and configuration note describes how to configure the Hypertext Transfer Protocol (HTTP) server and authentication login for the Catalyst Web Interface (CWI). It also describes how to download the Catalyst version of CiscoView (Catalyst CV) to your client.



**Note**

For the Catalyst 6500 series switches, the CWI is bundled with an online software image on Cisco.com. If your software image includes CWI, the name of the image contains “cv” appended to the supervisor engine. For example, an image for the Catalyst 6500 series switch is cat6000-sup2cvk8.8-1-3.bin.

---



**Note**

For the Catalyst 4500 series switches, the CWI is not bundled with an online software image on Cisco.com. You can download the CWI as a totally separate image from the supervisor engine software at the following URL: <http://www.cisco.com/cgi-bin/tablebuild.pl/cat4000>.

---



**Note**

For the Catalyst 5000 family switches, the CWI image is 8 MB. You must download the image to the PCMCIA card because it will not fit in the bootflash. You must also manually synchronize the CWI image to the standby supervisor engine.

---

## Contents

This document contains these sections:

- [Understanding How the CWI Works, page 2](#)
- [Hardware and Software Requirements, page 2](#)
- [Configuring the CWI, page 4](#)
- [Using the Catalyst CV, page 6](#)
- [Using CWI-Related CLI Commands, page 7](#)



---

Corporate Headquarters:  
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

Copyright © 2001–2003 Cisco Systems, Inc. All rights reserved.

# Understanding How the CWI Works

The CWI is a browser-based tool that you can use to configure the Catalyst 6500 series, Catalyst 4500 series, Catalyst 4000 series, Catalyst 5000 family, Catalyst 2948G, Catalyst 2948G-GE-TX, Catalyst 2980G, Catalyst 2980G-A, and Catalyst 4912G vmswitches. It consists of a graphical user interface (GUI) that runs on the client (Catalyst CV) and an HTTP server that runs on the switch.

The CWI provides a real-time graphical representation of the switch and detailed information, such as port status, module status, type of chassis, and modules.

Following a successful download, the Catalyst CV opens and displays switch information in your browser. The CWI obtains this information from the switch using SNMP requests.



**Note**

The CWI uses HTTP to download the Catalyst CV from the server to the client. HTTP is the TCP/IP protocol that the World Wide Web uses to exchange HTML documents.

Communication between the client and server usually occurs on a TCP/IP connection. The TCP/IP port number for HTTP is 80. In this client-server mode, the client opens a connection to the server and sends a request. The server receives the request, sends a response back to the client, and closes the connection.

The HTTP server supports the following requests:

- HTTP 0.9 (simple requests)
- HTTP 1.0 (full requests)
- HTTP 1.1 (full requests)

The HTTP server responds to a simple request with a simple response and to a full request with a full response.

In the default state, the HTTP server is disabled. To enable the CWI, you must enable the HTTP server. After you enable the HTTP server, it listens for requests on port number 80. You can change the TCP/IP port number to any port number from 1 to 65,535 at the CLI. If you change the TCP/IP port number that is not 80, then you will need to append the port number to the IP address of the switch. For example, if the IP address of the switch is `http://10.77.209.183`, and you change the TCP/IP port number to 900, then the URL for the switch will be `http://10.77.209.183:900`.

Although the system uses HTTP 1.0, it also supports HTTP 1.1 messaging.

## Hardware and Software Requirements

Table 1 shows the CWI hardware and software requirements.

*Table 1 CWI Hardware and Software Requirements*

Hardware and Software	Requirements
Supported Platforms	Catalyst 6000 and 6500 series—All supervisor engines Catalyst 5000 family—Supervisor Engine III and Supervisor Engine III F Catalyst 4003 series —Supervisor Engine I, Catalyst 4006, Catalyst 4500 series, Catalyst 2948G, 2948G-GE-TX, 2980G, 2980G-A, and 4912G —Supervisor Engine II

**Table 1** *CWI Hardware and Software Requirements (continued)*

Hardware and Software Requirements	
	Supervisor engine software release 5.4(2) or later release
	CV supervisor engine software release 5.5(8a) CV or later release is also required for the Catalyst 4000 series, Catalyst 4500 series, Catalyst 2948G, Catalyst 2980G, and Catalyst 4912 switches
	Supervisor engine software release 6.1(1) or later release and CV supervisor engine software 6.2(2a) CV or later for the Catalyst 2980G-A switch
	Supervisor engine software release 8.2(1)GLX or later release and the CV supervisor engine software release 8.2(1)GLX CV or later release for the Catalyst 2948G-GE-TX
Required Memory	<ul style="list-style-type: none"> <li>128 MB for the Catalyst 6500 series switches</li> </ul>
DRAM	<ul style="list-style-type: none"> <li>3.5 MB for the Catalyst 5000 family and Catalyst 2980G-A switches</li> <li>64 MB for the Catalyst 4000 series, Catalyst 4500 series, Catalyst 2948G, Catalyst 2948G-GE-TX, Catalyst 2980G, Catalyst 2980G-A, and Catalyst 4912G switches.</li> </ul> <p>Not a significant amount of memory is required for the HTTP server. The usage and performance impact depend on the number of concurrent HTTP sessions. The switch supports a maximum of three concurrent HTTP sessions.</p>
Flash	<ul style="list-style-type: none"> <li>17.5 MB for the Catalyst 6500 series switch with Supervisor Engine I</li> <li>13 MB for the Catalyst 6500 series switch with Supervisor Engine II</li> <li>18.5 MB for the Catalyst 6500 series switch with Supervisor Engine 720</li> <li>2.5 MB for the Catalyst CV files for the Catalyst 5000 family, Catalyst 4000 series, Catalyst 4500 series, Catalyst 2948G, Catalyst 2948G-GE-TX, Catalyst 2980G, and Catalyst 4912G switches (in addition to the switch image)</li> <li>40 KB for the HTTP server (in addition to the switch image)</li> </ul>
NVRAM	Not a significant amount of memory required for the CWI.
Required Disk Space	3.5 MB for the CWI (in addition to the switch image).

The supported client platforms, browsers, and Java Plug-in versions that are supported by CiscoView are as follows:

Client Platform	Web Browser	Java Plug-in
Solaris 2.7/2.8	Netscape Navigator 4.76, 4.77, 4.78, 4.79	Java Plug-in 1.3.0 (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)
Windows 98 Windows NT 4.0 Windows 2000	Internet Explorer 5.5 Netscape Navigator 4.76, 4.77, 4.78, 4.79	Java Plug-in 1.3.0-C (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)

Client Platform	Web Browser	Java Plug-in
HPUX 11.0	Netscape Navigator 4.77, 4.78, 4.79	Java Plug-in 1.2.2 (JRE 1.2.2) Java Plug-in 1.3.1 (JRE 1.3.1)
AIX 4.3.3	Netscape Navigator 4.77, 4.78, 4.79	Java Plug-in 1.3.0 (JRE 1.3.0) Java Plug-in 1.3.1 (JRE 1.3.1)



**Note** The Java Plug-in can be downloaded from this URL:  
<http://www.cisco.com/cgi-bin/tablebuild.pl/cview-plugin>



**Note** Java Plug-in versions 1.3.1\_01 and later are not supported by CWI.

## CWI Default Configuration

Table 2 shows the CWI default configuration.

*Table 2 CWI Default Configuration*

Feature	Default Value
HTTP server	Disabled
TCP/IP port number	80
Authentication	Enabled
HTTP trace	Disabled

## Configuring the CWI


Before you can access the Catalyst CV, you need to perform the tasks in these sections:

- [Configuring the HTTP Server, page 4](#)
- [Configuring Authentication Login, page 5](#)

## Configuring the HTTP Server

To configure the HTTP server, perform this task at the CLI:

	Task	Command
Step 1	Assign an IP address to the switch, if necessary.	<b>set interface sc0</b> [ <i>ip_addr / netmask</i> ]
Step 2	Enable the HTTP server on the switch.	<b>set ip http server enable</b>

	Task	Command
Step 3	Configure the HTTP port	<b>set ip http port <i>port_number</i> default</b>
	 <b>Note</b> The TCP/IP port default is 80; perform this step only if you need to change the default.	
Step 4	Verify the HTTP server and CWI support.	<b>show ip http</b>
Step 5	Display the CWI version.	<b>show version</b>
Step 6	Display the CWI configuration.	<b>show config</b>



**Note** The **show ip http** command displays the CWI status. If the switch supports the CWI, the “Web Interface” status field shows “Supported.” If the switch does not support the CWI, the field shows “Not Supported.”

## Configuring Authentication Login

The Catalyst switch software allows you to authenticate console and Telnet logins using the RADIUS/TACACS/Kerberos/Local database. With software release 5.4(2) or later releases, you can also authenticate HTTP users.

When you log into the switch using HTTP, a dialog box appears and prompts you for your username and password. After you provide your username and password, the system authenticates your login with the HTTP user-authentication method. The system denies access unless the username and password are valid.

In the default configuration, verification is enabled for all users of the CWI. The system validates the login password against the local login password.

Authentication for the CWI occurs at these two security levels:

- Level 1—Username and Password Authentication

Level 1 requires you to obtain authentication by providing a username and password. This process is similar to the authentication that you obtain at the command prompt for Telnet and console sessions.

After you pass the first level of security, you can download the Catalyst CV.

- Level 2—SNMP IP Permit Restriction

Level 2 restricts the IP address of the incoming SNMP request. You must configure the IP address of the SNMP request correctly before the CWI can communicate with the switch.



**Note** CWI does not support SNMP v3.

To configure authentication, perform this task at the CLI:

	Task	Command
Step 1	Configure authentication login.	<b>set authentication login enable</b> [console   telnet   http   all] [primary]
Step 2	Display authentication.	<b>show authentication</b>

This example shows how to configure the authentication login for the HTTP option:

```
Console> (enable) set authentication login tacacs enable http primary
Tacacs authentication set to enable for HTTP sessions as primary authentication method.
Console> (enable) set authentication login radius disable http primary
Tacacs authentication set to disable for HTTP sessions.
```

For detailed information on configuring the authentication login, refer to the “Configuring Switch Access Using AAA” chapter of the *Software Configuration Guide* for your switch.

## Downloading the Catalyst CV to the Client

To download the Catalyst CV from your browser, follow these steps:

- 
- Step 1** Enter the switch address in the URL field of your browser. For example, open Netscape Navigator or Internet Explorer and enter the following:
- ```
http://172.20.14.89
```
- In this example, 172.20.14.89 is the switch IP address.
- After you connect to the switch, a login dialog appears and prompts for your username and password.
- Step 2** Provide your username and password.
- The home page of the switch appears on your browser.
- Step 3** Click **Switch Manager** to download the Catalyst CV.
- The switch downloads the Catalyst CV, and your browser opens with a real-time view of the switch chassis.
- 



### Note

The CWI communicates with the switch through SNMP requests. If you enable the IP permit feature, you must set the IP address of the browser to “permitted” in the IP permit list for SNMP. For detailed information on configuring IP permit lists, refer to the “Configuring IP Permit List” chapter of the *Software Configuration Guide* for your switch.

---

## Using the Catalyst CV

The Catalyst CV is a subset of the CiscoView Network Management System. Most of the monitoring features that are available in CiscoView are not available in the Catalyst CV. For example, you cannot monitor CPU, port counters, or memory usage in the Catalyst CV. However, the Catalyst CV does provide a clear view of which ports are up and running and which ports are down.

**Note**

The non-embedded CiscoView (client/server CiscoView) can be launched from a device loaded with the CV image.

The primary purpose of the Catalyst CV is to provide a GUI to configure the switch for those customers who do not want to purchase the CiscoView Network Management System. For information on how to configure a Catalyst switch with the Catalyst CV, refer to the “Configuring Devices” chapter in the *CiscoView* documentation.

For documentation on how to use the Non-Embedded CiscoView, refer to the following URL:  
<http://www.cisco.com/en/US/partner/products/sw/cscowork/ps4565/index.html>.

## Using CWI-Related CLI Commands

The following sections describe how to use the CWI commands.

### Overview of the CLI Commands

Table 3 is an overview of the CLI commands for the CWI.

*Table 3* CLI Commands

| Command                                       | Functions                                |
|-----------------------------------------------|------------------------------------------|
| <b>set ip http server {enable   disable}</b>  | Configures the HTTP server on the switch |
| <b>set ip http port port_number   default</b> | Configures the HTTP port                 |
| <b>show ip http</b>                           | Displays the HTTP server information     |
| <b>show version</b>                           | Displays the CWI version number          |
| <b>show config</b>                            | Displays the CWI configuration           |
| <b>set authentication login</b>               | Configures the CWI authentication        |
| <b>show authentication</b>                    | Displays the CWI authentication          |

**Note**

For complete syntax and usage information for the commands used in this document, refer to the Command Reference for your switch.

### Configuring the HTTP Server

In the default state, the HTTP server is disabled on the switch. To configure the HTTP server, perform this task in privileged mode:

| Task                      | Command                                      |
|---------------------------|----------------------------------------------|
| Configure an HTTP server. | <b>set ip http server {enable   disable}</b> |

This example shows how to enable an HTTP server:

```
Console> (enable) set ip http server enable
HTTP server is enabled on the system.
```

This example shows the message that you receive when your switch does not support the CWI:

```
Console> (enable) set ip http server enable
Feature not supported on the system.
```

This example shows how to disable the HTTP server:

```
Console> (enable) set ip http server disable
HTTP server is disabled on the system.
```

## Configuring the HTTP Port

You do not need to use this command unless you want to change the default setting. In the default state, the TCP/IP port number on the server is 80. To configure the port number for the HTTP server, perform this task in privileged mode:

| Task                            | Command                                              |
|---------------------------------|------------------------------------------------------|
| Configuring the IP port number. | <b>set ip http port <i>port_number</i> / default</b> |

This example shows how to configure the TCP/IP port number to the default of 80:

```
Console> (enable) set ip http port default
HTTP TCP port number set to 80.
```

This example shows how to configure the TCP port number to 2398:

```
Console> (enable) set ip http port 2398
HTTP TCP port number set to 2398.
```

## Displaying the HTTP Server Information

To display the HTTP server information, perform this task in normal mode:

| Task                                 | Command             |
|--------------------------------------|---------------------|
| Display the HTTP server information. | <b>show ip http</b> |

This example shows how to view information on the HTTP server. This example shows a CWI that is supported:

```
Console> show ip http

HTTP Information:
-----
HTTP Server: enabled
HTTP port: 80
Web Interface: Supported
Web Interface version(s):
File: applet.html
CV stats: file /applet.html is padded, deducting
```



```

        size: 4791
File:   cvadp.jar
CV stats: file /cvadp.jar is padded, deducting
        size: 2164875
File:   cvadp_splash.jar
CV stats: file /cvadp_splash.jar is padded, deducting
        size: 19401
File:   cvadp_error.html
CV stats: file /cvadp_error.html is padded, deducting
        size: 401
        version: 8.1(1)
        date: 08/06.2003

```

HTTP active sessions: 0

Console> (enable)

This example shows how to display information on the HTTP server. This example shows a CWI that is not supported:

```

Console>(enable) show ip http
HTTP information:
-----
HTTP Server: disabled
HTTP port: 80
Web Interface: Not Supported

HTTP active sessions:
Console> (enable)

```

## Displaying the CWI Version Number

To display the CWI version number, perform this task in normal mode:

| Task                            | Command             |
|---------------------------------|---------------------|
| Display the CWI version number. | <b>show version</b> |

This example shows how to display the CWI version number:

```

Console> show version
WS-C4003 Software, Version NmpSW: 8.1(1)
Copyright (c) 1995-2003 by Cisco Systems, Inc.
NMP S/W compiled on Jul 25 2003, 07:46:52
GSP S/W compiled on Jul 25 2003, 03:52:03

System Bootstrap Version: 5.4(1)
System Web Interface Version: 8.1(1)

Hardware Version: 1.5  Model: WS-C4003  Serial #: JAB03130104

Mod Port Model                Serial #                Versions
-----
1   0   WS-X4012                JAB03130104           Hw : 1.5
                               Gsp: 8.1(1)
                               Nmp: 8.1(1)
2   48  WS-X4148                JAB023402QH           Hw : 1.0
3   6   WS-X4306                JAB024000YY           Hw : 0.2

```

```

          DRAM                FLASH                NVRAM
Module Total   Used   Free   Total   Used   Free   Total Used   Free
-----
1          65536K 37206K 28330K 12288K 10639K 1649K 480K 82K 398K

```

Uptime is 88 days, 21 hours, 40 minutes

## Displaying the CWI Configuration

To display the CWI configuration, perform this task in privileged mode:

| Task                           | Command            |
|--------------------------------|--------------------|
| Display the CWI configuration. | <b>show config</b> |

This example shows how to display the CWI configuration:

```

Console> (enable) show config
.....

.....

begin
!
# ***** NON-DEFAULT CONFIGURATION *****
!
!
#Time: Thu Sep 2 1999, 01:56:01
!
#version 5.4(0.74)MIA7-Eng
# System Web Interface Version 8.1(1)
!
! #!
#ip
set interface sc0 1 1.10.11.212/255.255.255.0 1.10.11.255

set ip route 192.168.242.0/255.255.255.0 1.10.11.1
!
#set boot command
set boot config-register 0x100
set boot system flash bootflash:cat6000-sup.5-2-1-CSX.bin
# HTTP commands
set ip http server enable
set ip http port 1922
!
#module 1 : 2-port 1000BaseX Supervisor
!
#module 2 empty
!
#module 3 : 48-port 10/100BaseTX (RJ-45)
set spantree portfast 3/8 enable
!
#module 4 empty
!
#module 5 : 48-port 10/100BaseTX (RJ-45)
!
#module 6 empty
!
end

```

## Configuring the Authentication Login

The **set authentication login** command includes the HTTP, Telnet, and console-session login options. For the HTTP option, you can configure the RADIUS, TACACS, or Kerberos authentication methods. If you configure the RADIUS authentication method for your HTTP session, then your username and password are validated using the RADIUS protocol. By default, the HTTP login is validated with the local login password.

To configure the authentication login for the HTTP option, perform this task in privileged mode:

| Task                                                    | Command                         |
|---------------------------------------------------------|---------------------------------|
| Configure the authentication login for the HTTP option. | <b>set authentication login</b> |

This example shows how to configure the authentication login for the HTTP option:

```
Console> (enable) set authentication login tacacs enable http primary
Tacacs authentication set to enable for HTTP sessions as primary authentication method.
Console> (enable) set authentication login radius disable http primary
Tacacs authentication set to disable for HTTP sessions.
```

## Displaying the Authentication

To display the authentication for the HTTP option, perform this task in privileged mode:

| Task                                        | Command                    |
|---------------------------------------------|----------------------------|
| Display authentication for the HTTP option. | <b>show authentication</b> |

This example shows how to display the HTTP authentication:

```
Console> (enable) show authentication

Login Authentication: Console Session  Telnet Session  Http Session
-----
tacacs                disabled        disabled        disabled
radius               disabled        disabled        enabled (primary)
kerberos             disabled        disabled        disabled
local                 enabled(primary)  enabled(primary)  enabled

Enable Authentication: Console Session  Telnet Session
-----
tacacs                disabled        disabled
radius               disabled        disabled
kerberos             disabled        disabled
local                 enabled(primary)  enabled(primary)
```

# 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](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](http://www.cisco.com/en/US/partner/ordering/ordering_place_order_ordering_tool_launch.html)

All users can order annual 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\\_inpk/pdi.htm](http://www.cisco.com/univercd/cc/td/doc/es_inpk/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, USA.) 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 send your comments in e-mail to [bug-doc@cisco.com](mailto: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

For all customers, partners, resellers, and distributors who hold valid Cisco service contracts, the Cisco Technical Assistance Center (TAC) provides 24-hour, award-winning technical support services, online and over the phone. Cisco.com features the Cisco TAC website as an online starting point for technical assistance.

### Cisco TAC Website

The Cisco TAC website (<http://www.cisco.com/tac>) provides online documents and tools for troubleshooting and resolving technical issues with Cisco products and technologies. The Cisco TAC website is available 24 hours a day, 365 days a year.

Accessing all the tools on the Cisco TAC website requires a Cisco.com user ID and password. If you have a valid service contract but do not have a login ID or password, register at this URL:

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

### Opening a TAC Case

The online TAC Case Open Tool (<http://www.cisco.com/tac/caseopen>) is the fastest way to open P3 and P4 cases. (Your network is minimally impaired or you require product information). After you describe your situation, the TAC Case Open Tool automatically recommends resources for an immediate solution. If your issue is not resolved using these recommendations, your case will be assigned to a Cisco TAC engineer.

For P1 or P2 cases (your production network is down or severely degraded) or if you do not have Internet access, contact Cisco TAC by telephone. Cisco TAC engineers are assigned immediately to P1 and P2 cases to help keep your business operations running smoothly.

To open a case 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 listing of Cisco TAC contacts, go to this URL:

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

## TAC Case Priority Definitions

To ensure that all cases are reported in a standard format, Cisco has established case priority definitions.

Priority 1 (P1)—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.

Priority 2 (P2)—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.

Priority 3 (P3)—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.

Priority 4 (P4)—You require information or assistance with Cisco product capabilities, installation, or configuration. There is little or no effect on your business operations.

## 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](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](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/index.html>



CCSP, CCVP, the Cisco Square Bridge logo, Follow Me Browsing, and StackWise are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, and iQuick Study are service marks of Cisco Systems, Inc.; and Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, the iQ logo, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, the Networkers logo, Networking Academy, Network Registrar, *Packet*, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, 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. (0502R)

Copyright © 2001—2003 Cisco Systems, Inc. All rights reserved.

 Printed in the USA on recycled paper containing 10% postconsumer waste.