



Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5)WC2b

February 2002

Cisco IOS Release 12.0(5)WC2b runs on Catalyst 2950 switches.

These release notes include important information about this IOS release and any limitations, restrictions, and caveats that apply to it. See the [“Related Documentation” section on page 27](#) for the complete list of Catalyst 2950 switch documentation.



Note

Before upgrading your switch to this release, read the [“Upgrading the Switch Software” section on page 19](#).

This IOS release is part of a special release of Cisco IOS software that is not released on the same 8-week maintenance cycle that is used for other platforms. As maintenance releases and future IOS releases become available, they will be posted to Cisco.com in the Cisco IOS software area.

Contents

This document has these sections:

- [“System Requirements” section on page 2](#)
- [“Features” section on page 5](#)
- [“Limitations and Restrictions” section on page 5](#)
- [“Documentation Notes” section on page 7](#)
- [“Caveats” section on page 8](#)
- [“Initial Configuration” section on page 14](#)
- [“Accessing CMS” section on page 17](#)
- [“Upgrading the Switch Software” section on page 19](#)
- [“Related Documentation” section on page 27](#)



Corporate Headquarters:

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

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

- [“Obtaining Documentation” section on page 27](#)
- [“Obtaining Technical Assistance” section on page 28](#)

System Requirements

This section describes these system requirements for IOS Release 12.0(5)WC2b:

- [“Hardware Supported” section on page 2](#)
- [“Software Requirements” section on page 2](#)

Hardware Supported

[Table 1](#) lists the Catalyst 2950 switches supported by this IOS release.

Table 1 Catalyst 2950 Switches

Switch	Description	Number of VLANs
Catalyst 2950-12	12 fixed autosensing 10/100 Ethernet ports	64
Catalyst 2950-24	24 fixed autosensing 10/100 Ethernet ports	64

Software Requirements

The minimum PC requirement is a Pentium processor running at 233 MHz with 64 MB of DRAM. The minimum UNIX workstation requirement is a Sun Ultra 1 running at 143 MHz with 64 MB of DRAM. [Table 2](#) lists the recommended platforms.

The following operating systems are supported for web-based management:

- Microsoft Windows 2000
- Microsoft Windows 95 (Service Pack 1 required)
- Microsoft Windows 98, second edition
- Microsoft Windows NT 4.0 (Service Pack 3 or higher required)
- Solaris 2.5.1 or higher, with the Sun-recommended patch cluster for that operating system and Motif library patch 103461-24

Table 2 Recommended Platform Configuration for Web-Based Management

OS	Processor Speed	DRAM	Number of Colors	Resolution	Font Size
Windows NT 4.0 ¹	Pentium 300 MHz	128 MB	65536	1024 x 768	Small
Solaris 2.5.1	Sparc 333 MHz	128 MB	Most colors for applications	—	Small (3)

1. Service Pack 3 or higher required

Browser Support

You can access the web-based interfaces through the browsers listed in [Table 3](#), which also lists the configuration that yields the best results for web-based management. The switch checks the browser version when starting a session to ensure that the browser is supported. If the browser is not supported, the switch displays an error message, and the session does not start.

Table 3 *Browser Support for Web-Based Management*

Browser	Minimum Version	Supported Versions
Netscape Communicator	4.61 ¹	4.61, 4.7x
Internet Explorer ²	4.01a	4.01a, 5.0

1. Netscape Communicator 4.6 and 6.0 are not supported.
2. Not supported on Solaris 2.5.1 or higher.



Note

In Cluster Management displays, Internet Explorer versions 4.01 and 5.0 might not display edge devices that are not connected to the command switch. Other functionality is similar to that of Netscape Communicator.

Installing the Required Plug-In

A browser Java plug-in is required to access the HTML-based Cluster Management Suite (CMS). Download and install the plug-in before you start CMS.

If the Java applet does not initialize after you have installed the plug-in, open the Java Plug-in Control Panel (**Start > Programs > Java Plug-in Control Panel**), and verify the following setting:

In the Proxies tab, verify that **Use browser settings** is checked and that no proxies are enabled.

If you are running McAfee VirusScan on Windows 2000 and the plug-in takes a long time to load, you can speed up CMS operation by disabling the VirusScan Internet Filter option, the Download Scan option, or both.

- From the Start menu, disable the options by selecting **Start > Programs > Network Associates > Virus Scan Console > Configure**.
- or
- From the task bar, right-click the Virus Shield icon, and in the Quick Enable menu, disable the options by deselecting **Internet Filter** or **Download Scan**.

Windows 2000, Windows 95, Windows 98, and Windows NT 4.0 Users

These Java plug-ins are supported on the Windows platform:



Caution

To avoid performance and compatibility issues, do not use Java plug-ins later than Java plug-in 1.3.0.

- Java plug-in JRE 1.2.2_05

If you start CMS without having installed the required Java plug-in, the switch automatically detects this. If you are using a supported Internet Explorer browser, it automatically downloads and installs the plug-in. If you are using a supported Netscape browser, the browser displays a Cisco.com (previously Cisco Connection Online [CCO]) page that contains the Java plug-in and installation instructions. If you are using Windows 2000, Netscape Communicator might not detect the missing Java plug-in. You can download the plug-in from one of these URLs:

- If you have a SmartNet support contract, download the plug-in from this URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/java>
- If you do not have a SmartNet contract, download the plug-in from this URL:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>

- Java plug-in JRE 1.3.0 (recommended)

This plug-in is not downloaded automatically. However, you can download it from this URL:

- If you have a SmartNet support contract, download the plug-in from this URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/java>
- If you do not have a SmartNet contract, download the plug-in from this URL:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>

**Note**

Uninstall older versions of the Java plug-in before installing the Java plug-in JRE 1.3.0.

Solaris Users

These Java plug-ins are supported on the Solaris platform:

**Caution**

To avoid performance and compatibility issues, do not use Java plug-ins later than Java plug-in 1.3.0.

- Java plug-in 1.2.2_05

This plug-in is supported, but not provided on the Cisco.com URL.

- Java plug-in 1.2.2_07 (recommended)
 - If you have a SmartNet support contract, download the plug-in from this URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/java>
 - If you do not have a SmartNet contract, download the plug-in from this URL:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>
- JRE 1.3.0
 - If you have a SmartNet support contract, download the plug-in from this URL:
<http://www.cisco.com/cgi-bin/tablebuild.pl/java>
 - If you do not have a SmartNet contract, download the plug-in from this URL:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/java>

Creating Clusters with Different Releases of IOS Software

Some versions of the Catalyst 2900 and 3500 XL software do not support clustering, and other versions do not support the features in this release. To ensure that all cluster switches are operating with the same level of software, we recommend that you upgrade all cluster switches to IOS Release 12.0(5.1)WC(1) or later.

If you have a cluster with switches that are running different versions of IOS software, changes on the latest release might not be reflected on switches running the older versions. For example, if you start Visual Switch Manager (VSM) on a switch running IOS Release 11.2(8)SA6, the windows and functionality can be different from a switch running IOS Release 12.0(5)WC2 or later.



Note

If your command switch is a Catalyst 2900 or 3500 XL switch running Cisco IOS Release 12.0(5.1)XW or earlier, a Catalyst 2950 switch will show as an unknown device in Cluster Manager. In this case, you will need to use Visual Switch Manager (VSM) to manage the Catalyst 2950 switch.

Features

For a detailed list of key features for this software release, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Limitations and Restrictions

Review this section before you begin working with the switches. Some features might not work as documented, and some features could be affected by recent changes to the switch hardware or software.

Connecting to the Cisco RPS 300

The Catalyst 2950 switches support the Cisco RPS 300 Redundant Power System.



Note

The Catalyst 2950 switches do not support the Cisco 600W Redundant Power System (RPS).

Port Configuration Conflicts

Certain combinations of port features create configuration conflicts (see [Table 4](#)). If you try to enable incompatible features, CMS issues a warning message, and you cannot make the change. Reload the page to refresh CMS.

In [Table 4](#), **No** means that the two referenced features are incompatible and should not both be enabled; **Yes** means that both can be enabled at the same time and will not cause an incompatibility conflict.

Table 4 *Conflicting Features*

	Protected Port	Port Group	Port Security	SPAN Port	Connect to Cluster?
Protected Port	–	Yes	Yes	No	Yes
Port Group	Yes	–	No	No	Yes
Port Security	Yes	No	–	No	Yes
SPAN Port	No	No	No	–	Yes
Connect to Cluster	Yes	Yes	Yes	Yes	–

Using Commas in CMS

Host names and Domain Name System (DNS) server names that contain commas on a cluster command switch, member switch, or candidate switch can cause CMS to behave unexpectedly. You can avoid this instability in the interface by not using commas in host names or DNS names. Also, do not enter commas when entering multiple DNS names in the IP Configuration tab of the IP Management window in CMS.

SPAN Limitations

When using the Switched Port Analyzer (SPAN) feature, the monitoring port receives copies of transmitted and received traffic for all monitored ports. If the monitoring port is 50 percent oversubscribed for a sustained period of time, it will probably become congested. One or more of the ports being monitored might also experience a slowdown.

Compatibility with the CiscoWorks2000 RME Suite

When using the Software Image Management (SWIM) application in the Resource Manager Essentials (RME) suite of the CiscoWorks2000 product family to perform automated system software and boot loader upgrades, you should note the following:

- Catalyst 2950 switches require IOS Release 12.0(5.2)WC(1) or later.
- Catalyst 2900 series XL switches require IOS Release 11.2(8)SA4 or later and RME version 2.1 or 2.2.
- Catalyst 3500 series XL switches require IOS Release 11.2(8.1)SA6 or later and RME version 2.2.

Ethernet Frame Size Support

The Catalyst 2950 switches support standard-size Ethernet frames (64 to 1518 bytes).



Note

Frame sizes larger than 1518 bytes are not supported.

Documentation Notes

All documentation for this release, except for these release notes, is provided on the *Catalyst 2950 Desktop Switch Documentation CD*.

Documentation CD

To view the contents of this documentation CD, double-click the index.htm file. Your browser will launch, and you will be able to select and view the documents on the CD.

If your PC is set to automatically launch CDs, the index page opens when you insert the CD or when you click the CD icon. If you need more information about how to set your PC to automatically launch CDs, consult your PC operating system documentation or systems administrator.



Note

From the .pdf files on the *Catalyst 2950 Desktop Switch Documentation CD*, clicking a link from the last page of the Table of Contents sometimes opens the Index instead of the section that you want. Another way to navigate to a section is to click a heading under the Bookmarks tab in the left window. To display subheadings, click the plus sign (+) next to the heading.

Correction to the Hardware Installation Guide

This information corrects an error in the *Catalyst 2950 Desktop Switch Hardware Installation Guide*.



Caution

Do not mount a Catalyst 2950 switch on a wall. Do not follow the mounting instructions as shown in Figure 2-6 on page 2-13 and Figure 2-7 on page 2-14 in the *Catalyst 2950 Desktop Switch Hardware Installation Guide*.

Correction to the Software Configuration Guide

This information corrects an error in Chapter 5, "Creating and Managing VLANs," of the *Catalyst 2950 Desktop Switch Software Configuration Guide*. In the "CLI: Configuring CoS Priority Queues" section, the CLI procedure to configure the CoS priority queues is described. The CLI command for Step 4 should be **show wrp-queue cos-map** instead of **show cos-map**.

Caveats

Open Caveats

This section describes possible unexpected activity by IOS Release 12.0(5)WC2b:

- CSCdt24814 (formerly CSCdt2481)

Source-based distribution port group does not share the broadcast with all the group members. When the destination of the packets is a broadcast or unknown unicast or multicast, the packets are forwarded only on one port member of a port group, instead of being shared among all members of the port group.

There is no workaround.

- CSCds72421

If you shut down the management VLAN on VLAN1 on a Catalyst 2950 switch, set the management VLAN to 999, and then again use the **shutdown** command to shut down VLAN1, the IP address of VLAN 999 does not appear in the **show cdp neighbor detail** command display on a connected device.

The workaround is to reboot the switch.

- CSCdt48011

There are two problems that occur when the Catalyst 2950 switch is in transparent mode:

- If the switch is a leaf switch, any new VLANs added to it are not propagated upstream through VTP messages. As a result, the switch does not receive flooded traffic for that VLAN.
- If the switch is connected to two VTP servers, it forwards their pruning messages. If the switch has a port on a VLAN that is not requested by other servers through their pruning messages, it does not receive flooded traffic for that VLAN.

There is no workaround.

- CSCds20365

Internal loopback in half-duplex mode causes input errors. We recommend that the PHY is configured to operate in full duplex before setting internal loopback.

There is no workaround.

- CSCdt83016

When the Catalyst 2950 switch boots up without being configured, it prompts the user with a configuration dialog. The switch allows the user to skip the dialog and to enable traps without configuring a community string. If the host trap receiver is configured without defining the community strings, when the switch attempts to generate a trap, it fails and displays an error message.

The workaround is to follow the configuration sequence by creating a community string before configuring traps for the host.

- CSCdr96565

Aging of dynamic addresses does not always occur exactly after the specified aging time elapses. It might take up to three times this time period before the entries are removed from the table.

There is no workaround.

- CSCdt74555

When a MAC address is learned on a member of a port group created between a Catalyst 2950 and Catalyst 2900 or 3500 XL switch, the same MAC address gets deleted and relearned on another port member of the port group on the 2900 or 3500 XL switch. As a result, a real-time diagnostic message reports this address relearning behavior. The symptom does not affect the connectivity and is informational only.

The workaround is to upgrade the image on the Catalyst 2900 or 3500 XL switch to the IOS Release 12.0(5.1)WC(1) or later.
- CSCdt48569

If any VLAN other than VLAN1 is configured as the management VLAN, the switch reports an incorrect shut down for VLAN1. VLAN1 is not administratively down even though the running configuration has shut down in VLAN1.

There is no workaround.
- CSCdt48351

The usage of the c2950BandwidthUsage Management Information Base (MIB) always shows zero, instead of displaying the current bandwidth usage statistics.

There is no workaround.
- CSCdt82729

If you launch the **VMPS Configuration** window from the device popup menu in Visual Switch Manager (VSM), it displays incorrect information.

The workaround is to not launch the **VMPS Configuration** window from the device popup menu, as VLAN Membership Policy Server (VMPS) is not supported on the Catalyst 2950 switches.
- CSCdt82712

If you launch VSM for a member switch, right-click the switch image to activate the device popup menu, and then left-click it to deactivate the popup menu, or if you select a port and deselect it, the Cluster Management icon on the toolbar is disabled and cannot be used to launch Cluster Management.

The workaround is to select **Cluster > Cluster Management** from the Cluster Management menu bar.
- CSCds68177

The UniDirectional Link Detection (UDLD) protocol does not always detect a unidirectional link when there is a loop between the TX and RX strands on the same port (TX/RX loop condition).

This is an intermittent problem, and there is no workaround.
- CSCds58369

If the switch gets configured from the dynamic IP pool, a duplicate or different IP address might be assigned.

The workaround is to make sure that the DHCP server contains reserved addresses that are bound to each switch by the switch hardware address so that the switch does not obtain its IP address from the dynamic pool.
- CSCdt49955

CMS dialogue windows can display two list selection boxes with **Add** and **Remove** buttons between them. If you press the Shift key on the keyboard at the same time as either the **Add** or **Remove** button, sometimes an exception error occurs. The exception error appears only inside the Java

console window and is not displayed by CMS. As a result of the exception error, the **Add** or **Remove** buttons might not function correctly. If you continue to click them, multiple entries are added to the available or selected list.

The workaround is to not hold down the Shift key when clicking **Add** or **Remove**.

- CSCdp67822

Cluster Management Suite requires a Java plug-in from Sun Microsystems. If you are using Internet Explorer and you disable Java plug-ins by using the Java Plug-In Control Panel, the initial Splash screen shows that the plug-in and Java are enabled, but Internet Explorer fails.

The workaround is to not disable Java plug-ins on the Java Plug-In Control Panel.

- CSCdp61365

If you right-click a device that is near the edge of the browser window, the second-level menu of the device pop-up menu might not display.

The workaround is to right-click again on the device until the pop-up menu displays correctly.

- CSCdp82224

The Cluster Manager System Time Management window supports the configuration of the Network Time Protocol (NTP) and system time. When you make changes on this window from a command switch, Java propagates the changes to all cluster members. A conflict can arise if you configure NTP and also use the Set Daylight Saving Time and Set Current Time tabs.

To avoid a possible conflict, either set the system time for the entire cluster on the command switch, or configure NTP on the command switch to use an NTP server to provide time to the cluster. Do not use both methods at the same time.

- CSCdp82354

You can use Cluster Manager to configure an Hot Standby Router Protocol (HSRP) standby group and bind it to a cluster. However, you cannot use Cluster Manager to configure more than one standby group. If you want to configure more than one standby group, use the command-line interface (CLI).

- CSCdp70389

When changing the management VLAN on a cluster with command-switch redundancy enabled, the cluster can break if HSRP is configured on any of the cluster members in the new management VLAN.

The workaround is to not change the management VLAN to a VLAN where a member is configured as part of a standby group.

- CSCdp85954

Root guard is inconsistent when configured on a port that is in the STP blocked state at the time of configuration.

- CSCdp49419

HSRP does not support a virtual MAC address entry or a built-in address (BIA) for a cluster.

- CSCdp97517

All members of an HSRP standby group must be cluster members.

- CSCdp30543

If the storm control filter is enabled for unicast, multicast, or broadcast traffic and the rising threshold is reached, all traffic on the port is filtered. No unicast, multicast, or broadcast traffic is forwarded from the port.

- CSCdp87748
Cisco IOS does perform some checks on entered IP addresses. For example, it does not allow the broadcast address to be entered. However, it does not check for the broadcast address on the same subnet as the HSRP Versatile Interface Processor (VIP) or the management VLAN IP address. This means that you could configure HSRP with a virtual IP address that is the same as the network broadcast address.
There is no workaround.
- CSCdp75220
If you use the command switch DNS server name to start CMS for a member that is running an earlier software release, CMS might not display the switch image, or it might display the command switch image. This can also occur when a standby group is configured for a cluster and you access CMS by entering the command-switch IP address and not the virtual IP address.
The workaround is to always use the command-switch IP address to access CMS. If a standby group is configured for a cluster, always use the virtual IP address to access CMS.
- CSCdp85928
CMS can behave unexpectedly if host names or DNS server names that it processes contain commas. This means that host names or DNS server names on a cluster command switch, member, or neighbor can cause instability in the HTML interface.
The workaround is to not include commas in host names or DNS server names in CMS.
- CSCdp62807
If you click the list of switches in CMS and press the Page Down key on the keyboard, the entire list moves to the bottom of the window. This only happens with Windows NT.
The workaround is to collapse the list into a single icon, which returns the list to the top of the window.
- CSCdp89945
In VSM, you cannot see the individual menu items when you right-click the chassis image to display the device pop-up menu.
The workaround is to right-click another part of the chassis image to display the device pop-up menu.

Resolved Caveats

These problems were resolved in Cisco IOS Release 12.0(5)WC2b:

- CSCdw65903
An error can occur with management protocol processing. Please use the following URL for further information:
<http://www.cisco.com/cgi-bin/Support/Bugtool/onebug.pl?bugid=CSCdw65903>
- CSCdw72113
A command switch no longer fails when it receives SNMP packets that have invalid variable bindings.

These problems were resolved in Cisco IOS Release 12.0(5)WC2:

- CSCdv35805
If you are copying the configuration file using `ciscoConfigCopyMIB` from a Catalyst 2950 switch by using Simple Network Management Protocol (SNMP) manager, the switch no longer reloads the configuration.
- CSCdv16305
A broadcast storm no longer occurs when two 100BASE-FX ports on a Catalyst 2950 switch are connected to the 100BASE-FX ports on another Catalyst 2950 switch if these ports are in trunk mode and one of the ports is administratively down.
- CSCds72421
If the management VLAN is changed to any other VLAN from VLAN 1 and VLAN 1 is shut down, the IP address configured in the new management VLAN now appears in the **show cdp neighbor detail** privileged EXEC command.
- CSCdt57346
When you use the **show rmon history** EXEC command, the value for the collision is now unique for each sample.
- CSCdu09410
The `ifSpeed` of the interfaces now reports the default value of the visible bandwidth when the link is down and reports the configured and assigned values when the link is up.
- CSCdu37367
The **clear counters** and **clear counters fastethernet <port>** interface commands now clear the port security counters. These commands also clear the other counters for the interface.
- CSCdu49099
Changing the VLAN Trunking Protocol (VTP) mode to transparent no longer causes a virtual type terminal session to lock up when executing commands, such as the **show vlan** privileged EXEC command, that require access to the VLAN- and VTP-related data.
In addition, ports that were shut down during VTP mode change now come back up automatically when VTP is stable.
- CSCdu67033
The output count displayed by the **show interface** privileged EXEC command output now displays correctly when the count is greater than 4,294,967,296 packets.
- CSCdu88701
When performing an **snmpwalk** SNMP operation on the `dot1dTpFdbTable` (1.3.6.1.2.1.17.4.3), the response no longer omits all entries of `show mac` in the display in which the first byte of the host MAC address is greater than 0x00.
- CSCdv21552
High CPU utilization no longer occurs when a switch boots with a VLAN (without an IP address) in the shutdown state while another active VLAN has an IP address.
- CSCdv41819
Enabling spanning-tree UplinkFast no longer causes brief spanning-tree loops if the configuration message from the root switch of the spanning tree ages out.

- CSCdt83016

When the Catalyst 2950 switch boots up without being configured, it prompts the user with a configuration dialog. The switch allows the user to skip the dialog and to enable traps without configuring a community string. If the host trap receiver is configured without defining the community strings, when the switch attempts to generate a trap, it fails and displays an error message.

The workaround is to follow the configuration sequence by creating a community string before configuring traps for the host.

- CSCdt04001

When you change the privilege level for interface on the Catalyst 2950 switches, you can execute commands with the newly configured privilege level. The switch now saves the arguments associated with the command, and after a reload, the configured commands are executable.

- CSCdt24089

If the Catalyst 2950 switch contains multicast addresses, the MIB walk of Dot1dTpFdbEntry no longer consumes excess CPU cycles on the switch.

- CSCdt68204

If you continuously ping a switch from a PC and the links from the switch to the network are brought down, when the link from the switch to the network is restored, pinging now resumes.

- CSCdt59751

The **no snmp-server enable traps snmp [authentication]** global configuration command is not supported by this software release.

- CSCdu87426

The 100BASE-FX ports in a Fast EtherChannel port group no longer loop packets when the connected device resets or reloads.

- CSCdv46396

If the switch has a MAC address of 00xx.xxxx.xxxx, it no longer halts after the **no port security** and **clear mac-address-table secure** commands are entered.

- CSCdv47498

The SNMP walk of the Dot1dTpFdbTable no longer causes the switch to halt and put an SNMP CPU HOG error message in the logging buffer.

- CSCdv51153

SNMP MIB variables etherStatsEntry does not display any values in Cisco IOS Release 12.0(5)XU or later.

There is no workaround.

This problem was resolved in Cisco IOS Release 12.0(5.3)WC(1):

- CSCdt88908

When IGMP packets are received on a port for a non-existent VLAN, the Catalyst 2950 switch no longer loses buffer space on that port.

Initial Configuration

You can assign IP information to your switch in these ways:

- Using the Setup program (switch's configuration dialog)
- Using DHCP-based auto configuration (refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*)
- Manually assigning an IP address (refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*)

Using the Setup Program

You can use an automatic setup program to assign switch IP information, host and cluster names, and passwords and to create a default configuration for continued operation. Later, you can use CMS or the command-line interface (CLI) to customize your configuration. To run the setup program, access the switch from the PC terminal that you connected to the console port. For information about connecting a PC or terminal to the switch console port, refer to the switch hardware installation guide.

The first time that you access the switch, it runs a setup program that prompts you for IP and other configuration information necessary for the switch to communicate with local routers and the Internet. This information is also required if you plan to use CMS to configure and manage the switch.



Note

If the switch will be a cluster member managed through the IP address of the command switch, it is not necessary to assign IP information or a password. If you are configuring the switch as a standalone switch or as a command switch, you must assign IP information.

You will need the following information from your system administrator:

Switch IP address _____

Subnet mask (netmask) _____

Default gateway (router) _____

Enable secret password _____

Use this procedure to create an initial configuration for the switch:



Note

Be sure the rollover cable is connecting a PC serial port to the switch console port. The data characteristics are 9600 baud, 8 data bits, 1 stop bit, and no parity. Use the supplied rollover cable and DB-9 adapter to connect a PC to the switch console port. You need to provide a RJ-45-to-DB-25 female DTE adapter if you want to connect the switch console port to a terminal. You can order a kit (part number ACS-DSBUASYN=) containing that adapter from Cisco. For console port and adapter pinout information, refer to the *Catalyst 2950 Desktop Switch Hardware Installation Guide*.

--- System Configuration Dialog ---

At any point you may enter a question mark '?' for help.
Use ctrl-c to abort configuration dialog at any prompt.
Default settings are in square brackets '[]'.

Step 1 Enter **Y** at the first prompt.

Continue with configuration dialog? [yes/no]: **y**

Step 2 Enter the switch IP address, and press **Return**:

Enter IP address: *ip_address*

Step 3 Enter the subnet mask, and press **Return**:

Enter IP netmask: *ip_netmask*

Step 4 Enter **Y** at the next prompt to specify a default gateway (router):

Would you like to enter a default gateway address? [yes]: **y**

Step 5 Enter the IP address of the default gateway, and press **Return**.

IP address of the default gateway: *ip_address*

Step 6 Enter a host name for the switch, and press **Return**.



Note

On a command switch, the host name is limited to 28 characters; on a member switch to 31 characters. Do not use *-n*, where *n* is a number, as the last character in a host name for any switch.

Enter a host name: *host_name*

Step 7 Enter a secret password, and press **Return**.



Note

The password can be from 1 to 25 alphanumeric characters, can start with a number, is case sensitive, allows spaces, but ignores leading spaces.

Enter enable secret: *secret_password*

Step 8 Enter **Y** to enter a Telnet password:

Would you like to configure a Telnet password? [yes] **y**



Note

The password can be from 1 to 25 alphanumeric characters, is case sensitive, allows spaces, but ignores leading spaces.

Step 9 Enter the Telnet password, and press **Return**:

Enter Telnet password: *telnet_password*

Step 10 Enter **Y** to configure the switch as the cluster command switch. Enter **N** to configure it as a member switch or as a standalone switch.

**Note**

If you enter **N**, the switch appears as a candidate switch in Cluster Builder. In this case, the message in Step 11 does not appear.

Would you like to enable as a cluster command switch? **y**

Step 11 Assign a name to the cluster, and press **Return**.

Enter cluster name: *cls_name*

**Note**

The cluster name can be 1 to 31 alphanumeric characters, dashes, or underscores.

Step 12 The initial configuration appears:

The following configuration command script was created:

```
ip subnet-zero
interface VLAN1
ip address 172.20.153.36 255.255.255.0
ip default-gateway 172.20.153.1
hostname host_name
enable secret 5 $1$M3pS$cXtAlkyR3/6Cn8/
line vty 0 15
password telnet_password
snmp community private rw
snmp community public ro
cluster enable cls_name

end
```

Step 13 Verify that the information is correct.

- If the information is correct, enter **Y** at the prompt, and press **Return**.
- If the information is not correct, enter **N** at the prompt, press **Return**, and begin again at Step 1.

Use this configuration? [yes/no]: **y**

After you complete the setup program, the switch can run the created default configuration. If you want to change this configuration or want to perform other management tasks, use one of these tools:

- CMS from your browser (See the [“Installing the Required Plug-In”](#) section on page 3 and the [“Accessing CMS”](#) section on page 17.)
- Command-line interface (CLI) (Refer to the software configuration guide.)

The switch software configuration guide provides more information about how to set a password to protect the switch against unauthorized Telnet access and how to access the switch if you forget the password.

Accessing CMS

A browser plug-in is required to access CMS. See the “[Installing the Required Plug-In](#)” section on [page 3](#). After you have assigned an IP address to the switch and installed the plug-in, you can access the switch from your browser and use the Cluster Management application to configure other switches. To use the web-based tools, see the “[Software Requirements](#)” section on [page 2](#) to set up the appropriate browser options.

Configuring Netscape Communicator (All Versions)

Follow these steps to configure Netscape Communicator:

-
- Step 1** Start Netscape Communicator.
 - Step 2** From the menu bar, select **Edit > Preferences**.
 - Step 3** In the Preferences window, click **Advanced**.
 - Step 4** Check the **Enable Java**, **Enable JavaScript**, and **Enable Style Sheets** check boxes.
 - Step 5** From the menu bar, select **Edit > Preferences**.
 - Step 6** In the Preferences window, click **Advanced Cache**, and select **Every time**.
 - Step 7** Click **OK** to return to the browser Home page.
-

Configuring Microsoft Internet Explorer (4.01)

Follow these steps to configure Microsoft Internet Explorer 4.01:

-
- Step 1** Start Internet Explorer.
 - Step 2** From the menu bar, select **View > Internet Options**.
 - Step 3** In the Internet Options window, click the **Advanced** tab.
 - a. Scroll through the list of options until you see Java VM. Check the **Java logging enabled** and **Java JIT compiler enabled** check boxes.
 - b. Click **Apply**.
 - Step 4** In the Internet Options window, click the **General** tab.
 - a. In the Temporary Internet Files section, click **Settings**.
 - b. In the Settings window, select **Every visit to the page**, and click **OK**.
-

Configuring Microsoft Internet Explorer (5.0)



Note

During the installation of this browser, make sure to check the **Install Minimal or Customize Your Browser** check box. In the Component Options window in the Internet Explorer 5 section, make sure to check the **Microsoft Virtual Machine** check box to display applets written in Java.

Follow these steps to configure Microsoft Internet Explorer 5.0:

-
- Step 1** Start Internet Explorer.
- Step 2** From the menu bar, select **Tools > Internet Options**.
- Step 3** In the Internet Options window, click the **Advanced** tab.
- Scroll through the list of options until you see Microsoft VM. Check the **Java logging enabled** and **JIT compiler for virtual machine enabled** check boxes.
 - Click **Apply**.
- Step 4** In the Internet Options window, click the **General** tab.
- In the Temporary Internet Files section, click **Settings**.
 - In the Settings window, select **Every visit to the page**, and click **OK**.

If you are using Microsoft Internet Explorer 5.0 to make configuration changes to the switch, note that this browser does not automatically reflect the latest configuration changes. Make sure you click the browser **Refresh** button for every configuration change.

Displaying the Access Page

After the browser is configured, display the Cluster Management Suite access page:

-
- Step 1** Enter the switch IP address in the browser **Location** field (Netscape Communicator) or **Address** field (Internet Explorer), and press **Return**.
- Step 2** Enter your username and password when prompted. The password provides level 15 access. The Cisco Systems Access page appears. For more information on Setting Passwords and Privilege Levels, refer to the *Catalyst 2950 Desktop Switch Software Configuration Guide*.
- Step 3** Click **Cluster Management Suite** or **Visual Switch Manager** to display the appropriate CMS application.
-

Upgrading the Switch Software

This section provides topics about upgrading the switch software:

- [“Guidelines for Upgrading Switch Software” section on page 19](#)
- [“Overview of the Switch Upgrade Process” section on page 19](#)
- [“Which Software Files to Download from Cisco.com” section on page 20](#)
- [“Downloading the New Software and TFTP Server Application to Your Management Station” section on page 21](#)
- [“Copying the Current Startup Configuration from the Switch to a PC or Server” section on page 21](#)
- [“Using Cluster Manager to Upgrade One or More Switches” section on page 22](#)
- [“Using the CLI to Upgrade a Catalyst 2950 Switch” section on page 23](#)
- [“Using the CLI to Upgrade Member Switches” section on page 25](#)



Note

Before upgrading your switch to Cisco IOS Release 12.0(5)WC2b, read the [“Guidelines for Upgrading Switch Software” section on page 19](#) for important information.



Note

For CMS instructions for upgrading switch software to this release, refer to the online help.

Guidelines for Upgrading Switch Software

When using Cluster Manager to upgrade multiple switches from the Cisco TFTP server, the Cisco TFTP server application can handle multiple requests and sessions. When using Cluster Manager to upgrade multiple switches from the Cisco TFTP server, you must first disable the **TFTP Show File Transfer Progress** and the **Enable Logging** options to avoid TFTP server failures. If you are performing multiple-switch upgrades with a different TFTP server, it must be capable of managing multiple requests and sessions at the same time.

Overview of the Switch Upgrade Process

The software upgrade procedure consists of these major steps:

- Deciding which software files to download from Cisco.com, as described in the [“Which Software Files to Download from Cisco.com” section on page 20](#).
- Downloading the combined .tar file from Cisco.com, as described in the [“Downloading the New Software and TFTP Server Application to Your Management Station” section on page 21](#). This file contains the IOS image and the HTML files. From Cisco.com, you can also download a TFTP server application to copy the switch software from your PC to the switch, if necessary.

The **tar** command extracts the IOS image and the HTML files from the combined .tar file during the TFTP copy to the switch.

- Copying the current startup configuration file, as described in the [“Copying the Current Startup Configuration from the Switch to a PC or Server” section on page 21](#). If the upgrade to the new software fails or if the new startup configuration fails, you can reinstall the previous version of the switch software and use the copy of the startup configuration file to start the switch. If a failure

occurs while copying a new image to the switch, and the old image has already been deleted, you will need to use the XMODEM protocol to recover an image for the switch. For more information, refer to the “Recovering from Corrupted Software” section in the “Troubleshooting” chapter of the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

- Using CMS or the CLI to upgrade the software on your switch or switch cluster:
 - If you are using Cluster Manager to upgrade a switch, follow the steps in the [“Using Cluster Manager to Upgrade One or More Switches”](#) section on page 22.
 - If you are using the CLI to upgrade a switch, follow the steps in the [“Using the CLI to Upgrade a Catalyst 2950 Switch”](#) section on page 23, or [“Using the CLI to Upgrade Member Switches”](#) section on page 25.

When you upgrade a switch, the switch continues to operate while the new software is copied to Flash memory. If Flash memory has enough space, the new image is copied to the selected switch but does not replace the running image until you reboot the switch. If a failure occurs during the copy process, you can still reboot your switch by using the old image. If Flash memory does not have enough space for two images, the new image is copied over the existing one. Features provided by the new software are not available until you reload the switch.

Which Software Files to Download from Cisco.com

New software releases are posted on Cisco.com and are also available through authorized resellers.

[Table 5](#) describes the file extensions and what they mean for the upgrade procedure. It is easier to upgrade the switch software by using a combined .tar file that contains the HTML files and the IOS image. The upgrade procedures in these release notes describe how to perform the upgrade by using a combined .tar file, and you must use a combined .tar file to upgrade a switch through the CMS.

[Table 6](#) lists the software files for this IOS release.



Note

We recommend that you download the combined .tar file that contains the IOS image file and the HTML files. The procedures in these release notes are for upgrading a switch by using the combined .tar file, and the VSM and Cluster Manager are designed to upgrade a switch by using this combined file.

Table 5 Possible Extensions for IOS Software Files

Extension	Description
.tar	A compacted file from which you can extract files by using the tar command. There are two types of .tar files: <ul style="list-style-type: none"> • A <i>combined .tar</i> file that contains both the IOS image file and the HTML files. • An <i>HTML .tar</i> file that has the letters <i>HTML</i> in its name and contains just the HTML files for the IOS release. From the CLI, you can upgrade the switch software by using this HTML file and the IOS image file.
.bin	The IOS image file that you can copy to the switch through TFTP.

Table 6 Catalyst 2950 Cisco IOS Software Files

Filename	Description
c2950-c3h2s-mz.120-5.WC2b.bin	IOS image file
c2950-c3h2s-mz.120-5.WC2b.tar	IOS image file and HTML files

Downloading the New Software and TFTP Server Application to Your Management Station

Follow these steps to download the new software and, if necessary, the TFTP server application, from Cisco.com to your management station:

-
- Step 1** Use [Table 5](#) and [Table 6](#) to identify the files that you want to download.
- Step 2** Download the files from one of these locations:
 If you have a SmartNet support contract, go to this URL, and download the appropriate files:
<http://www.cisco.com/cgi-bin/tablebuild.pl/cat2950>
 If you do not have a SmartNet contract, go to this URL, and download the appropriate files:
<http://www.cisco.com/pcgi-bin/tablebuild.pl/cat2950>
- Step 3** Use the CLI or web-based interface to perform a TFTP transfer of the file or files to the switch after you have downloaded them to your PC or workstation.
 The readme.txt file describes how to download the TFTP server application. New features provided by the software are not available until you reload the software.
-

Copying the Current Startup Configuration from the Switch to a PC or Server

When you make changes to a switch configuration, your changes become part of the running configuration. When you enter the command to save those changes to the startup configuration, the switch copies the configuration to the config.text file in Flash memory. To ensure that you can recreate the configuration if a switch fails, you might want to copy the config.text file from the switch to a PC or server.

The following procedure requires a configured TFTP server such as the Cisco TFTP server available on Cisco.com.

Beginning in privileged EXEC mode, follow these steps to copy a switch configuration file to the PC or server that has the TFTP server application:

-
- Step 1** Copy the file in Flash memory to the root directory of the TFTP server:
`switch# copy flash:config.text tftp`
- Step 2** Enter the IP address of the device where the TFTP server resides:
`Address or name of remote host []? ip_address`

Step 3 Enter the name of the destination file (for example, **config.text**):

Destination filename [config.text]? yes/no

Step 4 Verify the copy by displaying the contents of the root directory on the PC or server.

Using Cluster Manager to Upgrade One or More Switches

You can use the Software Upgrade feature of the Cluster Manager to upgrade all or some of the switches in a cluster at once. Consider the following conditions when doing an upgrade:

- You cannot upgrade Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches at the same time. However, you can group together and upgrade Catalyst 1900 and Catalyst 2820 switches at the same time.
- Upgrade Catalyst 1900 and Catalyst 2820 switches last. To function efficiently, these switches need to be rebooted shortly after the upgrade occurs. If you do not click **Reboot Cluster** in 30 seconds after the upgrade, the Catalyst 1900 and Catalyst 2820 switches automatically reboot.
- For Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches, enter the *image_name.tar* filename in the New File Name field. The .tar file contains both the IOS image and the web-management code.
- For Catalyst 1900 and Catalyst 2820 switches, enter the *image_name.bin* filename in the New File Name field. The .bin file contains the software image and the web-management code.

Follow these steps to use Cluster Manager to upgrade software. Refer to the online help for more details.

Step 1 In Cluster Manager, select **System > Software Upgrade** to display the Software Upgrade window.

Step 2 Enter the .tar filename (for Catalyst 2950, Catalyst 2900 XL and Catalyst 3500 XL switches) or the .bin filename (for Catalyst 1900 and Catalyst 2820 switches) that contains the switch software image and the web-management code.

You can enter just the filename or a pathname into the **New Image File Name** field. You do not need to enter a pathname if the image file is in the directory that you have defined as the TFTP root directory.



Note

You can also use Visual Switch Manager (VSM) to upgrade a single switch by following the same software upgrade procedure.



Note

Close your browser after the upgrade process is complete.

On Catalyst 2950, Catalyst 2900 XL, and Catalyst 3500 XL switches, new images are copied to Flash memory and do not affect operation. The switch checks Flash memory to ensure that there is sufficient space before the upgrade takes place. If there is enough space, the new image is copied to the switch without replacing the old image, and after the new image is completely downloaded, the old one is erased. In this case, you can still reboot your switch by using the old image if a failure occurs during the copy process.

If there is not enough space in Flash memory for the new and old images, the old image is deleted, and the new image is downloaded.

**Note**

If a failure occurs while copying a new image to the switch, and the old image has already been deleted, you need to use the XMODEM protocol to recover an image for the switch. For more information, refer to the “Recovering from Corrupted Software” section in the “Troubleshooting” chapter of the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

Using the CLI to Upgrade a Catalyst 2950 Switch

This procedure is for upgrading Catalyst 2950 switches by copying the combined .tar file to the switch. You copy the files to the switch from a TFTP server and extract the files by entering the **tar** command, with the following results:

- Changes the name of the current image file to the name of the new file that you are copying and replaces the old image file with the new one.
- Disables access to the HTML pages and deletes the existing HTML files before the software upgrade to avoid a conflict if users access the web pages during the software upgrade.
- Reenables access to the HTML pages after the upgrade is complete.

Follow these steps to upgrade the switch software by using a TFTP transfer:

Step 1 If your PC or workstation cannot act as a TFTP server, copy the file to a TFTP server to which you have access.

Step 2 Access the CLI by starting a Telnet session or by connecting to the switch console port through the RS-232 connector.

To start a Telnet session on your PC or workstation, enter the following command:

```
server% telnet switch_ip_address
```

Enter the Telnet password if you are prompted to do so.

Step 3 Enter privileged EXEC mode:

```
switch> enable  
switch#
```

Enter the password if you are prompted to do so.

Step 4 Display the name of the running (default) image file (BOOT path-list). The following example shows the name in *italic*:

```
switch# show boot  
BOOT path-list:    flash:current_image  
Config file:      flash:config.text  
Enable Break:     1  
Manual Boot:      no  
HELPER path-list:  
NVRAM/Config file  
buffer size: 32768
```

Step 5 If there is no software image defined in the BOOT path-list, enter **dir flash:** to display the contents of Flash memory.

- Step 6** Using the exact, case-sensitive name of the combined .tar file that you downloaded, rename the running image file to that name, and replace the .tar extension with .bin. The image filename is then the same as the downloaded filename but with a .bin extension. This step does not affect the operation of the switch.

```
switch# rename flash:current_image flash:new_image
Source filename [current_image]?
Destination filename [new_image]?
```

For example:

```
switch# rename flash:c2950-c3h2s-mz.120-5.WC2.bin flash:c2950-c3h2s-mz.120-5.WC2b.bin
```

- Step 7** Display the contents of Flash memory to verify the renaming of the file:

```
switch# dir flash:
Directory of flash:/

Directory of flash:/
 3  drwx      10176   Mar 01 2001 00:04:34  html
 6  -rwx       2343   Mar 01 2001 03:18:16  config.text
171 -rwx      1667997   Mar 01 2001 00:02:39  c2950-c3h2s-mz.120-5.WC2b.bin
 7  -rwx       3060   Mar 01 2001 00:14:20  vlan.dat
172 -rwx        100   Mar 01 2001 00:02:54  env_vars

7741440 bytes total (4788224 bytes free)
```

- Step 8** Enter global configuration mode:

```
switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

- Step 9** Disable access to the switch HTML pages:

```
switch(config)# no IP http server
```

- Step 10** Enter the **boot** command with the name of the new image filename:

```
switch(config)# boot system flash:new_image
```

For example:

```
switch(config)# boot system flash:c2950-c3h2s-mz.120-5.WC2b.bin
```



Note If the **show boot** command entered in [Step 4](#) displays no image name, you do not need to enter this command; the switch automatically finds the correct file to use when it resets.

- Step 11** Return to privileged EXEC mode:

```
switch(config)# end
```

- Step 12** Remove the HTML files:

```
switch# delete flash:html/*
```

Press **Enter** to confirm the deletion of each file. Do not press any other keys during this process.



Caution In the following step, the **tar** command copies the combined .tar file that contains both the image and the HTML files. You do *not* need to copy an HTML .tar file in this procedure.

Step 13 Enter the following command to copy the new image and HTML files to Flash memory:

```
switch# tar /x tftp://server_ip_address//path/filename.tar flash:
Loading /path/filename.tar from server_ip_address (via VLAN1):!
extracting info (110 bytes)
extracting c2950-c3h2s-mz.120-5.WC2b.bin (7741440 bytes)!!!!!!!!!!!!!!!!!!!!!!
html/ (directory)
extracting html/Detective.html.gz (1139 bytes)!
extracting html/ieGraph.html.gz (553 bytes)
extracting html/DrawGraph.html.gz (787 bytes)
extracting html/GraphFrame.html.gz (802 bytes)!
...
```

Depending on the TFTP server being used, you might need to enter only one slash (/) after the *server_ip_address* in the **tar** command.

Step 14 Enter global configuration mode:

```
switch# config terminal
Enter configuration commands, one per line. End with CNTL/Z.
```

Step 15 Re-enable access to the switch HTTP pages:

```
switch(config)# IP http server
```

Step 16 Return to privileged EXEC mode:

```
switch(config)# end
```

Step 17 Reload the new software with the following command:

```
switch# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

Step 18 Press **Return** to confirm the reload.

Your Telnet session ends when the switch resets.

After the switch reboots, use Telnet to return to the switch, and enter the privileged EXEC mode **show version** command to verify the upgrade procedure. If you have a previously opened browser session to the upgraded switch, close the browser, and start it again to ensure that you are using the latest HTML files.

Using the CLI to Upgrade Member Switches

Because a member switch might not be assigned an IP address, command-line software upgrades through TFTP are managed through the command switch.

This section provides these procedures:

- [“Upgrading Catalyst 2950, Catalyst 2900 XL or Catalyst 3500 XL Member Switches” section on page 26](#)
- [“Upgrading Catalyst 1900 or Catalyst 2820 Member Switches” section on page 26](#)

Upgrading Catalyst 2950, Catalyst 2900 XL or Catalyst 3500 XL Member Switches

Follow these steps to upgrade the software on a member switch:

- Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, select the number of the member switch that you want to upgrade. The member number is in the SN column of the display. You need this member number for Step 2.

- Step 2** Log in to the member switch (for example, member number 1):

```
switch# rcommand 1
```

- Step 3** Start the TFTP copy function as if you were initiating it from the command switch.

```
switch-1# tar /x tftp://server_ip_address//path/filename.tar flash:
Source IP address or hostname [server_ip_address]?
Source filename [path/filename]?
Destination filename [flash:new_image]?
Loading /path/filename.bin from server_ip_address (via!)
[OK - 843975 bytes]
```

- Step 4** Reload the new software with the following command:

```
switch-1# reload
System configuration has been modified. Save? [yes/no]:y
Proceed with reload? [confirm]
```

Press **Enter** to start the download.

You lose contact with the switch while it reloads the software. For more information on the **rcommand**, refer to the *Catalyst 2950 Desktop Switch Command Reference*.

Upgrading Catalyst 1900 or Catalyst 2820 Member Switches

Follow these steps to upgrade the software on a Catalyst 1900 or Catalyst 2820 member switch:

- Step 1** In privileged EXEC mode on the command switch, display information about the cluster members:

```
switch# show cluster members
```

From the display, select the number of the member switch that you want to upgrade. The member number is in the SN column of the display. You need this member number for Step 2.

- Step 2** Log in to the member switch (for example, member number 1):

```
switch# rcommand 1
```

- Step 3** For switches running standard edition software, enter the password (if prompted), access the Firmware Configuration menu from the menu console, and perform the upgrade. Follow the instructions in the installation and configuration guide that shipped with your switch. When the download is complete, the switch resets and begins using the new software.

The Telnet session accesses the menu console (the menu-driven interface) if the command switch password is privilege level 15. If the command switch password is privilege level 1, you are prompted for the password.

You lose contact with the switch while it reloads the software.

- Step 4** For switches running Enterprise Edition Software, start the TFTP copy as if you were initiating it from the member switch:

```
switch-1# copy tftp://host/src_file opcode
```

For example, **copy tftp://spaniel/op.bin opcode** downloads new system operational code *op.bin* from the host *spaniel*.

You should see the `TFTP successfully downloaded operational code` message. When the download is complete, the switch resets and begins using the new software. If this message does not appear, refer to the installation and configuration guide that shipped with your switch for more information.

You can also upgrade the switch software through the Firmware Configuration menu from the menu console. For more information, refer to the installation and configuration guide that shipped with your switch.

You lose contact with the switch while it reloads the software.

Related Documentation

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the “[Obtaining Documentation](#)” section on page 27.

These publications provide more information about the switches:

- The *Catalyst 2950 Desktop Switch Software Configuration Guide* (order number DOC-7811380=)
- The *Catalyst 2950 Desktop Switch Command Reference* (order number DOC-7811381=)
- The *Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)
- *Catalyst GigaStack Gigabit Interface Converter Hardware Installation Guide* (DOC-786460=)
- Cluster Management Suite (CMS) online help

Obtaining Documentation

The following sections explain how to obtain documentation from Cisco Systems.

World Wide Web

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

<http://www.cisco.com>

Translated documentation is available at the following URL:

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

Documentation CD-ROM

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

Ordering Documentation

Cisco documentation is available in the following ways:

- Registered Cisco Direct Customers can order Cisco product documentation from the Networking Products MarketPlace:
http://www.cisco.com/cgi-bin/order/order_root.pl
- Registered Cisco.com users can order the Documentation CD-ROM through the online Subscription Store:
<http://www.cisco.com/go/subscription>
- Nonregistered Cisco.com users can order documentation through a local account representative by calling Cisco corporate headquarters (California, USA) at 408 526-7208 or, elsewhere in North America, by calling 800 553-NETS (6387).

Documentation Feedback

If you are reading Cisco product documentation on Cisco.com, you can submit technical comments electronically. Click **Leave Feedback** at the bottom of the Cisco Documentation home page. After you complete the form, print it out and fax it to Cisco at 408 527-0730.

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

To submit your comments by mail, use the response card behind the front cover of your document, or write to the following address:

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

We appreciate your comments.

Obtaining Technical Assistance

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

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information, networking solutions, services, programs, and resources at any time, from anywhere in the world.

Cisco.com is a highly integrated Internet application and a powerful, easy-to-use tool that provides a broad range of features and services to help you to

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

You can self-register on Cisco.com to obtain customized information and service. To access Cisco.com, go to the following URL:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC is available to all customers who need technical assistance with a Cisco product, technology, or solution. Two types of support are available through the Cisco TAC: the Cisco TAC Web Site and the Cisco TAC Escalation Center.

Inquiries to Cisco TAC are categorized according to the urgency of the issue:

- Priority level 4 (P4)—You need information or assistance concerning Cisco product capabilities, product installation, or basic product configuration.
- Priority level 3 (P3)—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- Priority level 2 (P2)—Your production network is severely degraded, affecting significant aspects of business operations. No workaround is available.
- Priority level 1 (P1)—Your production network is down, and a critical impact to business operations will occur if service is not restored quickly. No workaround is available.

Which Cisco TAC resource you choose is based on the priority of the problem and the conditions of service contracts, when applicable.

Cisco TAC Web Site

The Cisco TAC Web Site allows you to resolve P3 and P4 issues yourself, saving both cost and time. The site provides around-the-clock access to online tools, knowledge bases, and software. To access the Cisco TAC Web Site, go to the following URL:

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

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

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

If you cannot resolve your technical issues by using the Cisco TAC Web Site, and you are a Cisco.com registered user, you can open a case online by using the TAC Case Open tool at the following URL:

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

If you have Internet access, it is recommended that you open P3 and P4 cases through the Cisco TAC Web Site.

Cisco TAC Escalation Center

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

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

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

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

This document is to be used in conjunction with the documents listed in the "Related Documentation" section.



Copyright © 2001–2002, Cisco Systems, Inc.
All rights reserved.