



Release Notes for the Catalyst 2950 Cisco IOS Release 12.0(5.2)WC(1)

April 2001

Cisco IOS Release 12.0(5.2)WC(1) runs on Catalyst 2950 switches.



Note

The documentation shipped with the Catalyst 2950 switches refers to Release 12.0(5)WC(1). The correct IOS release is IOS Release 12.0(5.2)WC(1). For a complete list of these documents, see the [“Documentation Notes” section on page 7](#).

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 17](#) for the complete list of Catalyst 2950 switch documentation.

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 the following 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 7](#)
- [“Initial Configuration” section on page 12](#)
- [“Accessing CMS” section on page 15](#)
- [“Recovering from Software Failure” section on page 17](#)
- [“Related Documentation” section on page 17](#)



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

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

78-11693-02

- [“Obtaining Documentation” section on page 17](#)
- [“Obtaining Technical Assistance” section on page 19](#)

System Requirements

This section describes these system requirements for IOS Release 12.0(5.2)WC(1):

- [“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
Catalyst 2950C-24	24 fixed autosensing 10/100 Ethernet ports and 2 100BASE-FX ports	64
Catalyst 2950T-24	24 fixed autosensing 10/100 ports and 2 fixed autosensing 10/100/1000 Ethernet ports ¹	64

1. The Gigabit Ethernet ports can operate in either half- or full-duplex mode when they are set to 10 or 100 Mbps, but when they are set to 1000 Mbps, they can operate only in full-duplex mode.

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 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

There are two Java plug-ins that are supported on these platforms:



Note

We recommend using Java plug-in JRE 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/cat2950>

- If you do not have a SmartNet contract, download the plug-in from this URL:

<http://www.cisco.com/pcgi-bin/tablebuild.pl/cat2950>

- Java plug-in JRE 1.3.0

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

<http://www.cisco.com/cgi-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

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



Note

We recommend using JRE 1.2.2_07.

- JRE 1.2.2_07

You need to install the Java plug-in *and* the JRE 1.2.2_07:

- Download and install the Java plug-in for Solaris from this URL:

<http://www.sun.com/software/solaris/netscape/jpis/>

- Install the JRE 1.2.2_07 from this URL:

<http://www.sun.com/software/solaris/java/download.html>

Follow the links in the section titled J2SE: Java 2 Standard Edition (1.2.2_07 Localized) for the JRE 1.2.2_7 plug-in instructions.

- JRE 1.3.0

The JRE 1.3.0 does not require you to download a separate Java plug-in as it is included with the JRE 1.3.0. Download and install the JRE 1.3.0 for Solaris from this URL:

<http://www.cisco.com/cgi-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(5.2)WC(1) 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

This section should be reviewed 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*.

References to IOS Release Number

These documents refer to Cisco IOS Release 12.0(5)WC(1). The correct IOS release is Cisco IOS Release 12.0(5.2)WC(1).

- *Catalyst 2950 Desktop Switch Software Configuration Guide Cisco IOS Release 12.0(5)WC(1)*
- *Catalyst 2950 Desktop Switch Command Reference Cisco IOS Release 12.0(5)WC(1)*
- *Catalyst 2950 Desktop Switch Hardware Installation Guide*

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*.

Caveats

This section describes possible unexpected activity by IOS Release 12.0(5.2)WC(1).

- CSCdt24089

If the Catalyst 2950 switch contains multicast addresses, the MIB walk of Dot1dTpFdbEntry can be inefficient, sometimes consuming excess CPU cycles on the switch.

There is no workaround.

- CSCdt88908

If IGMP packets are received on a port for a non-existent VLAN, the Catalyst 2950 switch loses buffer space on that port. The switch supports only 64 VLANs; therefore, this only occurs if the Catalyst 2950 switch is connected to a switch that has more than 64 VLANs configured.

There is no workaround.
- CSCdt24814

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.
- CSCdt04001

On the Catalyst 2950 switches, when the privilege level is changed for the interface, commands can be executed with the newly configured privilege level. However, the switch does not save the arguments associated with the command, and after a reload, the configured commands are not executable.

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. (CSCdt48569)
- CSCdt57346

When you use the **show rmon history** command, the value for the collision is cumulative instead of being unique for each sample. The value for a collision in a given sample can be calculated by subtracting from the previous sample.

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.
- CSCdt18106

The snmpwalk on the Catalyst 2950 CISCO-IP-STAT-MIB loops continuously when using IP accounting precedence on VLANs other than VLAN1.

The workaround is to use individual **snmpget** requests to retrieve data.
- CSCdt68204

If you continuously ping a switch from a PC and the links from the switch to the network are brought down, one link from the switch to the network is restored, ping does not resume.

The workaround is to run the **clear cam** command.
- 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
The DHCP server should contain 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. If the switch gets configured from the dynamic IP pool, a duplicate or different IP address might be assigned.
- 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 is displayed 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 crashes.
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.

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 also is 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 is not displayed.

```
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 is displayed:

```
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 15)

- 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 select 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.
- a. Scroll through the list of options until you see Java VM. Check the **Java logging enabled** and **JIT compiler for virtual machine 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 the **Settings**.
 - b. 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.
-

Recovering from Software Failure

In the event of a software failure you can reload the software. For detailed recovery procedures, refer to the “Troubleshooting” chapter in the *Catalyst 2950 Desktop Switch Software Configuration Guide*.

The software files for this IOS release are listed in [Table 5](#):

Table 5 *Catalyst 2950 Switches Cisco IOS Software Files*

Filename	Description
c2950-c3h2s-mz.120-5.2.WC.1.bin	IOS image-only file
c2950-c3h2s-mz.120-5.2.WC.1.tar	IOS image and HTML files
c2950-html-plus.120-5.2.WC.1.tar	HTML files

Related Documentation

You can order printed copies of documents with a DOC-xxxxxx= number. For more information, see the “[Obtaining Documentation](#)” section on page 17.

The following publications provide more information about the switches:

- Catalyst 2950 Desktop Switch Documentation CD

This CD is shipped with the switch and contains the following documents:

- The *Catalyst 2950 Desktop Switch Software Configuration Guide, Cisco IOS Release 12.0(5)WC(1)* (order number DOC-7811380=)
- The *Catalyst 2950 Desktop Switch Command Reference, Cisco IOS Release 12.0(5)WC(1)* (order number DOC-7811381=)
- The *Catalyst 2950 Desktop Switch Hardware Installation Guide* (order number DOC-7811157=)



Note These documents refer to Cisco IOS Release 12.0(5)WC(1). The correct IOS release is Cisco IOS Release 12.0(5.2)WC(1).

- Cluster Management Suite (CMS) online help

Obtaining Documentation

The following sections provide sources for obtaining documentation from Cisco Systems.

World Wide Web

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

- <http://www.cisco.com>
- <http://www-china.cisco.com>
- <http://www-europe.cisco.com>

Documentation CD-ROM

Cisco documentation and additional literature are available in a CD-ROM package, which ships 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 as 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, in North America, by calling 800 553-NETS(6387).

Documentation Feedback

If you are reading Cisco product documentation on the World Wide Web, you can send us your comments by completing the online survey. When you display the document listing for this platform, click **Give Us Your Feedback**. If you are using the product-specific CD and you are connected to the Internet, click the pencil-and-paper icon in the toolbar to display the survey. After you display the survey, select the manual that you wish to comment on. Click **Submit** to send your comments to the Cisco documentation group. You can e-mail your comments to bug-doc@cisco.com.

To submit your comments by mail, for your convenience many documents contain a response card behind the front cover. Otherwise, you can mail your comments to the following address:

Cisco Systems, Inc.
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. For Cisco.com registered users, additional troubleshooting tools are available from the TAC website.

Cisco.com

Cisco.com is the foundation of a suite of interactive, networked services that provides immediate, open access to Cisco information and resources at anytime, from anywhere in the world. This highly integrated Internet application is a powerful, easy-to-use tool for doing business with Cisco.

Cisco.com provides a broad range of features and services to help customers and partners streamline business processes and improve productivity. Through Cisco.com, you can find information about Cisco and our networking solutions, services, and programs. In addition, you can resolve technical issues with online technical support, download and test software packages, and order Cisco learning materials and merchandise. Valuable online skill assessment, training, and certification programs are also available.

Customers and partners can self-register on Cisco.com to obtain additional personalized information and services. Registered users can order products, check on the status of an order, access technical support, and view benefits specific to their relationships with Cisco.

To access Cisco.com, go to the following website:

<http://www.cisco.com>

Technical Assistance Center

The Cisco TAC website is available to all customers who need technical assistance with a Cisco product or technology that is under warranty or covered by a maintenance contract.

Contacting TAC by Using the Cisco TAC Website

If you have a priority level 3 (P3) or priority level 4 (P4) problem, contact TAC by going to the TAC website:

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

P3 and P4 level problems are defined as follows:

- P3—Your network performance is degraded. Network functionality is noticeably impaired, but most business operations continue.
- P4—You need information or assistance on Cisco product capabilities, product installation, or basic product configuration.

In each of the above cases, use the Cisco TAC website to quickly find answers to your questions.

To register for Cisco.com, go to the following website:

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

If you cannot resolve your technical issue by using the TAC online resources, Cisco.com registered users can open a case online by using the TAC Case Open tool at the following website:

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

Contacting TAC by Telephone

If you have a priority level 1 (P1) or priority level 2 (P2) problem, contact TAC by telephone and immediately open a case. To obtain a directory of toll-free numbers for your country, go to the following website:

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

P1 and P2 level problems are defined as follows:

- P1—Your production network is down, causing a critical impact to business operations if service is not restored quickly. No workaround is available.
- P2—Your production network is severely degraded, affecting significant aspects of your business operations. No workaround is available.

This document is to be used in conjunction with the documents listed in the “[Related Documentation](#)” section.

AccessPath, AtmDirector, Browse with Me, CCDA, CCDE, CCDP, CCIE, CCNA, CCNP, CCSI, CD-PAC, *CiscoLink*, the Cisco *NetWorks* logo, the Cisco *Powered* Network logo, Cisco Systems Networking Academy, the Cisco Systems Networking Academy logo, Fast Step, Follow Me Browsing, FormShare, FrameShare, GigaStack, IGX, Internet Quotient, IP/VC, iQ Breakthrough, iQ Expertise, iQ FastTrack, the iQ Logo, iQ Net Readiness Scorecard, MGX, the Networkers logo, *Packet*, PIX, RateMUX, ScriptBuilder, ScriptShare, SlideCast, SMARTnet, TransPath, Unity, Voice LAN, Wavelength Router, and WebViewer are trademarks of Cisco Systems, Inc.; Changing the Way We Work, Live, Play, and Learn, Discover All That’s Possible, and Empowering the Internet Generation, are service marks of Cisco Systems, Inc.; and Aironet, ASIST, BPX, Catalyst, Cisco, the Cisco Certified Internetwork Expert logo, Cisco IOS, the Cisco IOS logo, Cisco Systems, Cisco Systems Capital, the Cisco Systems logo, Enterprise/Solver, EtherChannel, EtherSwitch, FastHub, FastSwitch, IOS, IP/TV, LightStream, MICA, Network Registrar, Post-Routing, Pre-Routing, Registrar, StrataView Plus, Stratm, SwitchProbe, TeleRouter, and VCO are registered trademarks of Cisco Systems, Inc. and/or its affiliates in the U.S. and certain other countries.

All other brands, names, or trademarks mentioned in this document or Web site 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. (0103R)

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